105i-H-2

MAY 2 1 1988

Y3.N88:10/1217

NUREG-1217

Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants

Technical Findings Related to Unresolved Safety Issue A-47

Draft Report for Comment

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

A. J. Szukiewicz

ORIGINAL

COMPLETED

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Information Support Services, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG-1217

Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants

Technical Findings Related to
Unresolved Safety Issue A-47

Draft Report for Comment

Manuscript Completed: March 1988
Date Published: April 1988

A. J. Szukiewicz

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

This report summarizes the work performed by the Nuclear Regulatory Commission staff and its contractors, Idaho National Engineering Laboratories (INEL), Oak Ridge National Laboratory (ORNL), and Pacific Northwest Laboratory (PNL), leading to the proposed resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The technical findings and conclusions presented in this document are based on the technical work completed by the contractors. The principal documents that contain the technical findings and conclusions of the contractors for USI A-47 are summarized in Appendix B.

An in-depth evaluation was performed on non-safety-grade control systems (see Section 1) that are typically used during normal plant operation on four nuclear steam system (NSS) plants: a General Electric Company (GE) boiling-water reactor (BWR), a 3-loop Westinghouse (W) pressurized-water reactor (PWR) design, a once-through steam generator PWR designed by Babcock and Wilcox Co. (B&W), and a Combustion Engineering (CE) PWR design. A study was also conducted to determine the generic applicability of the results to the class of plants represented by the specific plants analyzed. Generic conclusions were then developed.

Steam generator and reactor vessel overfill events and reactor vessel overcool events were identified as major classes of events having the potential to be more severe than previously analyzed. Specific subtasks of this issue were to study these events to determine the need for preventive and/or mitigating design measures.

The impact of the Rancho Seco event (December 26, 1985) which involved a loss of power to the integrated control system (ICS) is also discussed. This effort is closely coordinated with the USI A-47 effort, but is being evaluated separately by the B&W Owners Group and the NRC staff. Any requirements developed will be imposed independently of USI A-47.

This report describes the technical studies performed by the laboratories, the NRC staff assessment of the results, the generic applicability of the evaluations, and the technical findings resulting from these studies.

BLANK PAGE

TABLE OF CONTENTS

		Page
ABSTRACT		iii
ACKNOWLEDGEMENTS		ix
ABBREVIATIONS		xi
1	STATEMENT OF THE ISSUE	1-1 1
2	APPROACH	2-1 4
2.1	Selection of Plants	2-1 4
2.2	Limitations and Assumptions of the Study	2-1 4
2.3	USI A-47 Program Overview	2-3 6
2.4	Review Procedures	2-5 8
2.4.1	Criteria Development	2-5 8
2.4.2	Systems Level Failure Mode and Effects Analyses	2-6 9
2.4.3	Thermal-Hydraulic Transient Analyses	2-6 9
2.4.4	Literature Search	2-8 11
2.4.5	Failure Analyses of Significant Control System Failures	2-8 11
3	RESULTS OF THE INEL AND ORNL STUDIES	3-1 16
3.1	Potentially Significant Control System Failure Scenarios	3-1 16
3.1.1	GE BWR Plant	3-1 16
3.1.2	W 3-Loop PWR Plant	3-1 16
3.1.3	B&W PWR Plant	3-2 17
3.1.4	CE PWR Plant	3-2 17
3.2	Literature Search	3-3 18
3.2.1	GE BWR Plants	3-3 18
3.2.2	W PWR Plants	3-4 19
3.2.3	B&W PWR Plants	3-4 19
3.2.4	CE PWR Plants	3-4 19
4	GENERIC APPLICABILITY	4-1 33
4.1	GE BWR Plants	4-2 34
4.1.1	Overfill Events at Power Resulting From Failures in the Reactor Vessel High-Level Feedwater Trip System	4-3 35
4.1.2	Overfill and Overcool Events During Low-Pressure Startup and Shutdown Operations	4-5 37

TABLE OF CONTENTS (Continued)

		Page
4.2	W PWR Plants	4-6 38
4.2.1	Overfill Events Resulting From a Sustained Operation of the Auxiliary Feedwater Flow	4-6 38
4.2.2	Overfill Events Resulting From Failures in the Steam Generator, High-Level, Feedwater, Trip System	4-8 40
4.2.3	Overcool Events During Hot Shutdown and Full-Power Operation	4-9 41
4.2.4	Overpressure Events During Low-Temperature and Low-Pressure Shutdown or Startup Operating Conditions	4-11 43
4.2.5	Control System Failures Aggravating a Steam Generator Tube Rupture Event	4-13 45
4.3	B&W PWR Plants	4-14 46
4.3.1	Overfill Events Resulting From Failures in the Steam Generator, High-Level, Main-Feedwater, Trip System	4-14 46
4.3.2	Overheat Events Resulting From Steam Generator Dryout	4-16 48
4.4	CE PWR Plants	4-17 49
4.4.1	Overfill Events Resulting From Operator Errors During a Steam Generator Overfeed Event	4-18 50
4.4.2	Overheat Events and Possible Pressurized Thermal Shock Events Resulting From Operator Errors During Small-Break Loss-of-Coolant Accidents	4-19 51
5	SUMMARY AND CONCLUSIONS	5-1 53
6	REFERENCES	6-1 55

APPENDIX A: OTHER RELATED STUDIES, PROGRAMS, AND ISSUES
APPENDIX B: SUMMARY OF THE PRINCIPAL DOCUMENTS USED FOR USI A-47 STUDY

LIST OF TABLES

		Page	
2.1	Control system screening criteria used by INEL to identify potentially significant control system failures on the GE BWR reference plant design.....	2-10	13
2.2	Control system screening criteria used by INEL to identify potentially significant control system failures on the W PWR reference plant design.....	2-11	14
2.3	Control system screening criteria used by ORNL to identify potentially significant control system failures on the B&W and CE PWR reference plant designs.....	2-12	15
3.1	Potentially significant failure scenarios in a representative GE BWR.....	3-5	20
3.2	Potentially significant failure scenarios in a representative W PWR.....	3-7	22
3.3	Potentially significant failure scenarios in a representative B&W PWR.....	3-12	27
3.4	Potentially significant failure scenarios in a representative CE PWR.....	3-15	30

BLANK PAGE

ACKNOWLEDGEMENTS

The technical findings relevant to Unresolved Safety Issue A-47, "Safety Implications of Control Systems," which are presented in this report, represent the combined efforts of staffs at the Nuclear Regulatory Commission, INEL - Idaho, ORNL - Tennessee [and ORNL's subcontractor Science Applications Inc. (SAI)], and PNL - Richland, Washington. The following individuals deserve special mention for their participation and contributions:

N. Anderson	NRC/RES
W. Bickford	PNL
S. Bruske	INEL
W. Hodges	NRC/NRR
E. Lantz	NRC/NRR
A. McBride	SAI
C. Ransome	INEL
R. Stone	ORNL

BLANK PAGE

ABBREVIATIONS

ADV	atmospheric dump valve
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ATWS	anticipated transients without scram
B&W	Babcock and Wilcox Co.
BWR	boiling-water reactor
CE	Combustion Engineering
CFR	Code of Federal Regulations
CSF	control system failure
CSI	core spray injection
CSS	core spray system
ECC	emergency core cooling
ECCS	emergency core cooling system
EFW	emergency feedwater
FMEA	failure mode and effects analysis
FSAR	final safety analysis report
GE	General Electric Co.
HPI	high-pressure injection
IEEE	Institute of Electrical and Electronics Engineers
INEL	Idaho National Engineering Laboratories
LCO	limiting condition for operation
LER	licensee event report
LOCA	loss-of-coolant accident
LPCI	low-pressure coolant injection
LTOP	low-temperature overpressure
MFW	main feedwater
MMS	modular modeling system
MSIV	main steam isolation valve
MSIB	main steam line break
NRC	U.S. Nuclear Regulatory Commission
NSS	nuclear steam system
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
PNL	Pacific Northwest Laboratory
PORV	power-operated relief valve

PRA	probabilistic risk analysis
PTS	pressurized thermal shock
PWR	pressurized-water reactor
RCS	reactor coolant system
SAI	Science Applications Inc.
SAR	safety analysis report
SBLOCA	small-break LOCA
SGTR	steam generator tube rupture
SIAS	safety injection actuation signal
SRV	safety/relief valve
TBV	turbine bypass valve
TMI	Three Mile Island
UCLA	University of California at Los Angeles
USI	Unresolved Safety Issue
W	Westinghouse Corp.

1 STATEMENT OF THE ISSUE

Nuclear power plant instrumentation and control systems comprise safety-grade protection systems and non-safety-grade control systems. The safety-grade protection systems are designed to satisfy the general design criteria (GDC) identified in 10 CFR Part 50 and are used to (1) trip the reactor whenever certain specific parameters exceed allowable limits, (2) protect the core from overheating by initiating the emergency core cooling systems, and (3) actuate other safety systems such as the closure of main steam isolation valve or opening of the safety or relief valves to maintain the plant in a safe condition. Non-safety-grade control systems are used to maintain a nuclear plant within prescribed pressure and temperature limits during shutdown, startup, and normal power operation. Non-safety-grade control systems are not relied on to perform any safety functions during or following postulated accidents. They are used to control plant processes that could have a significant impact on the plant dynamics. Non-safety-grade control systems include, but are not limited to: (1) reactivity control systems, (2) reactor coolant pressure, temperature, level, and flow control systems, and (3) inventory control systems (such as feedwater and borated water controls). In addition, they include secondary system pressure and flow controls (pressurized-water reactor) as well as associated support systems, such as electric, hydraulic, and pneumatic power supply systems. The non-safety-grade control systems are not required to be designed to satisfy the GDC.

During the licensing review processes, the NRC performs an audit review on the non-safety-grade instrumentation and control systems, on a case-by-case basis. Although this audit review is not conducted to the same degree as the review of the safety systems, the reviews provide confidence that an adequate degree of separation and independence is provided between these non-safety-grade systems and the safety-grade protection systems. The audit reviews also provide confidence that misoperation or failure of non-safety-grade control systems does not result in transient conditions more severe than conditions assumed in the bounding analyses reported in the plant Safety Analysis Report (SAR).

Events that licensees are required to address are specified in Chapter 15 of the Standard Review Plan (NRC, NUREG-0800). These events include, but are not limited to:

(1) feedwater system malfunctions that result in a decrease or an increase in the feedwater flow (including the loss of normal feedwater flow)

(2) steam pressure regulator malfunctions or failures that result in an increase or a decrease in the steam flow (including the turbine trip event)

(3) spectrum of reactivity addition events

(4) chemical and volume control malfunctions that increase the reactor coolant inventory or decrease the boron concentration

Because non-safety-grade control systems are only audited as part of the licensing review, there may exist some potential (which an audit review did not disclose) for accidents or transients developing into more severe events than previously analyzed, if compounded by non-safety-grade control system failures.

These system failures or malfunctions may occur independently or as a result of an accident or transient. Concerns have previously been identified [NRC (AEOD), 1980, NUREG-0153) in which a failure or malfunction of the non-safety-grade control system can (1) potentially cause a steam generator or reactor vessel to overfill (see AEOD report) or (2) can lead to a transient (in pressurized-water reactors) in which the vessel could be subjected to severe overcooling (see NRC, SECY-82-465). In addition, the potential exists for a single failure (such as a loss of power supply, a short circuit, an open circuit, a control sensor failure) or for multiple failures resulting from a common-cause failure to cause a malfunction of one or more control systems which could lead to an undesirable control system response, or could provide misleading information to the plant operator.

The purpose of the Unresolved Safety Issue (USI) A-47 study is to perform a more in-depth review of the non-safety-grade control systems and to (1) evaluate the need for modifying control systems in operating reactors, (2) verify the adequacy of current licensing requirements identified in Section 7.7 of the Standard Review Plan (NRC, NUREG-0800), and (3) evaluate the need for additional guidelines and criteria to ensure that non-safety-grade control system failures do not pose unacceptable public risk. To this end, tasks were established to identify control systems whose failure could (1) cause transients or accidents to be potentially more severe than those identified in the final safety analysis report (FSAR) and previously analyzed, (2) adversely affect any assumed or anticipated operator action during the course of transients or accidents, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents to occur at a frequency in excess of those established for abnormal operational transients and design-basis accidents.

It should be noted that the focus of the USI A-47 review was directed to identify and evaluate control system failures that could cause transients or accidents to be potentially more severe than those identified in the FSAR. Control system failure-induced transients that were bounded by the FSAR analysis were not considered significant failures for this review. These transients were evaluated, but if they were determined to be adequately mitigated by safety-grade systems or if sufficient time was available for the transients to be mitigated by subsequent operator action and not exceed the bounding analyses, they were not considered to pose an important risk to public health and safety.

Because control systems are an integral part of plant operations, failures in these systems have historically caused plants to shut down or to actuate safety systems. Challenges to the safety systems could represent a small but potentially significant fraction of the overall plant risk. This fact has been demonstrated in plant probabilistic risk assessments that have been performed to date. As a result of plant-specific analyses that have exposed unique vulnerabilities to severe accidents, some plants have modified their designs. Generally, undesirable contributions to risk have been reduced to acceptable levels by changing procedures or modifying designs. The Commission plans to

formulate an integrated systematic approach to examine the design of each nuclear power plant now operating or under construction for significant risk contributors. Once NRC and the nuclear industry have developed a method of analysis, every nuclear power plant that has not yet been appropriately examined will be studied, and any changes that are needed will be made to ensure that there is no excessive risk to public health and safety (NRC, NUREG-1070).

The section that follows, "Approach," describes (1) the approach used to review non-safety-grade control systems, (2) the limitations and assumptions made, and (3) the methods developed and the activities performed. Section 3 describes the results of the individual plant reviews and identifies the control system failure scenarios determined to be potentially safety significant. Section 4 discusses the generic applicability of the plant-specific reviews of the reference plants, Section 5 presents the staff's conclusions, and Section 6 lists the references cited in this report. Appendix A provides a summary of other NRC and industry studies, programs, and issues related to USI A-47. In Appendix B, the principal documents underlying the proposed resolution of USI-A-47 are summarized.

2 APPROACH

2.1 Selection of Plants

Three pressurized-water reactor (PWR) plant designs and one boiling-water reactor (BWR) plant design were selected for the review of non-safety-grade control systems. These reference plants are specific designs from each of the four major nuclear steam supply system (NSSS) suppliers: Babcock and Wilcox Co. (B&W), Westinghouse Corp. (W), Combustion Engineering Co. (CE), and General Electric Co. (GE). A major factor in the selection of the reference plants was the quality and quantity of plant-specific design information available to the NRC staff. In addition, the three PWR designs were already being evaluated in the study of USI A-49, "Pressurized Thermal Shock," and a significant amount of information obtained in that study could be utilized. The BWR plant was selected because a considerable amount of design information was available from other NRC projects. Also, an existing thermal-hydraulic computer model was available for this plant.

The reference plant designs were reviewed by two national laboratories. Two of the PWR plants, representing B&W and CE designs, were evaluated by Oak Ridge National Laboratory (ORNL) (NRC, NUREG/CR-4047, -4265 (Vols. 1 & 2), -4449). The other two plant designs, a GE BWR and a W PWR design, were evaluated by Idaho National Engineering Laboratory (INEL) [NRC, NUREG/CR-4262 (Vols. 1 & 2), -4326 (Vols. 1 & 2)]. The risk analyses for potentially significant control system failures were performed by Pacific Northwest Laboratory (PNL) (NRC, NUREG/CR-4387, -4385, -4386, -3958). Appendix B summarizes the content of the principal documents used for this review.

2.2 Limitations and Assumptions of the Study

To perform a systematic review of control system failures, it became quickly evident that the scope of the review had to be confined. The type of events and the type, number, and combinations of possible control system failures were therefore limited. In order to limit the review to a manageable level, limitations and assumptions had to be made. These limitations and assumptions and their bases are discussed below.

(1) Non-safety-grade control system failures would not cause simultaneous failure of both redundant trains of safety-grade protection systems. This assumption implies that a minimum number of safety-grade protection systems would be available for (a) actuation of the reactor trip system, (b) actuation of the overpressure protection system, and (c) initiation of the minimum number of required emergency core cooling (ECC) systems, if needed during a control system failure transient. This assumption is considered valid on the basis that adequate separation and independence is required to be provided between the non-safety-grade control systems and the safety-grade protection systems. Independence is provided by verifiable isolation devices located between safety-grade and non-safety-grade systems and/or by physically locating the safety systems in separate areas and routing the electrical cables in separate raceways throughout the plant. The staff

audits the safety-grade systems (audit reviews) as part of the licensing review process to ensure that an adequate degree of separation and independence has been provided. Also, as part of the A-47 program, a literature search was conducted to review the operating history of control system failures. The purpose of the review, in part, was to identify any control system failures that could cause a failure in both safety-grade protection systems. The staff's review (see Section 3.2 of this report) did not identify any such failures. In addition, as part of the USI A-17, systems interactions program, spatial interactions between safety-grade systems and non-safety-grade systems were considered. Any identified interactions between safety-grade systems and non-safety-grade control systems were evaluated.

(2) External events such as earthquakes, floods, fires, and sabotage have not been considered in this study. Multiple control system failures were evaluated to assess some effects of common-cause failures on the plant. However, the review was limited to a selected number of control system failure combinations. Not all control system failures that could occur as a result of these external events were reviewed in detail. An attempt was made to select those failure scenarios that would bound the dynamic effects of a number of control system failures. System failures were evaluated for automatic and manual modes of operation and at different reactor power levels that included low-, intermediate-, and full-power operation.

It should be noted that evaluations by the staff and the utilities have been performed to assess the plant's ability to achieve safe shutdown during these external events. Fire protection reviews for all operating plants have also been performed to assure conformance to 10 CFR Part 50 Appendix R and to evaluate the plant's ability to cope with fires and flooding in different cable trays as well as in different areas of the plant. These reviews evaluated the effects of fires and flooding in control-grade as well as protection-grade equipment.

Also, as part of the USI A-46 activities, control-grade and protection-grade equipment are evaluated to assess their seismic ruggedness and assure that plants have the ability to achieve safe shutdown after a design-basis seismic event (see item 2 in Appendix A to this report).

(3) Operator errors of omission or commission were not addressed in this review. Operating procedures for the important transients were reviewed. An assessment was made to determine whether operating procedures (to mitigate the transients of concern) were written so that the operator could accomplish the task in the time allowed. An evaluation was also performed to determine whether there was sufficient information (i.e., alarms and/or indications) available in the control room for the operator to assess the conditions in the plant at the time of the event. In some cases, early recognition of transients was necessary. Given early recognition, there were actions that the operator could take to mitigate these events. For the purposes of developing the failure scenarios and analyzing resulting transients on the plant model, two of the four reviews assumed no operator action for the first 10 minutes of the transient. The other plant reviews evaluated operator action on the basis of available time for action during each transient. For the risk analysis phase evaluating the core-melt

frequency, operator action for all plants reviewed was determined on the basis of available time for action during each significant transient identified.

(4) Transients resulting from control system failures during limiting conditions for operation (LCOs) (for example, systems deliberately disabled for a short time for testing and/or maintenance) were not considered in the review.

(5) The processes used to modify and to maintain control systems were not considered in this review.

(6) Anticipated transients without scram (ATWS) were not considered in the review. A separate generic study (NRC, NUREG-0460) was conducted to address this issue. On July 25, 1984, Title 10 of the Code of Federal Regulations (CFR) was amended to include Section 50.62 (ATWS Rule) which requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the likelihood of failure to shut down the reactor following anticipated transients and to mitigate the consequences of an ATWS envent.

(7) Control system failures that could lead to failures of liquid tanks located outside containment and to fuel handling accidents (for example, spent fuel or accidents involving waste disposal systems) were not considered in this review. These systems do not usually interface with control systems that are used during normal plant operations.

(8) Individual utilities had to address IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," and to modify their plants appropriately in order to ensure that the operator would be able to achieve cold shutdown conditions after a loss of power of a single bus to instrumentation and controls in systems used in attaining cold shutdown. A reevaluation of IE Bulletin 79-27 regarding the consequences of a loss of power to the instrumentation and control systems is currently being performed for all B&W-designed operating plants (see item 5 in Appendix A to this report).

(9) The items of NUREG-0737, "Clarification of TMI Action Plan Requirements" (November 1980), were implemented or committed to be implemented on individual plant designs, including but not limited to Items II.E.1.1, II.E.1.2, II.K.2.2, II.K.2.9, and II.G.1.

2.3 USI A-47 Program Overview

Figure 2.1 summarizes the A-47 program and identifies that program's major activities. Both INEL and ORNL concentrated on identifying control system failures that could lead to:

(1) steam generator (reactor vessel) overfill events
(2) reactor vessel overcooling events
(3) reactor core overheating events
(4) events or accidents that could be more severe than those previously analyzed in the FSAR

Steam generator and reactor vessel overfill and reactor vessel overcool events have been identified previously as potentially significant transients that could lead to unacceptable consequences. Review of how control system failures contribute to these events was, therefore, a major part of the program. The methodology developed during this phase of the review was then applied to identifying and evaluating control system failures contributing to reactor core overheating events and events or accidents that could be more severe than those previously analyzed in the FSAR.

The goal of the review was to identify the non-safety-grade control systems whose failure or misoperation could:

(1) cause transients or accidents identified in the FSAR analysis of the reference plants to be potentially more severe than previously analyzed,

(2) adversely affect any assumed or anticipated operator action during the course of a particular event,

(3) cause technical specification safety limits to be exceeded,

(4) cause transients or accidents to occur at a frequency in excess of the values established for abnormal operational transients and design-basis accidents,

(5) cause frequent challenges to the protection systems.

INEL and ORNL developed similar approaches for evaluating control systems. Each approach consisted of several activities conducted in parallel:

(1) Selection criteria for choosing important systems and important failure sequences were developed.

(2) Failure mode and effects analyses were performed for all control systems in each reference plant to (a) identify systems that had the potential to affect the events of concern (that is, overfill, overcool, overheat, etc.) and (b) identify the failure modes that would aggravate the events.

(3) A literature search was conducted to review the operating history of selected plants and identify system failures that adversely affected plant safety.

(4) Thermal-hydraulic computer models (for each reference plant design) were developed with sufficient detail of the plant systems and control systems design to simulate the dynamic responses of the plant during transient conditions.

(5) Analysis was verified by comparing selected transient response calculations with actual plant data and other independent analyses using accepted and verified codes.

Credible combinations as well as some highly unlikely failure combinations of systems were analyzed to identify important control system failure sequences and to evaluate their consequences. Non-safety-grade control system failures were evaluated for automatic and manual modes of operation and at different

reactor power levels (low-, intermediate-, and full-power operations) in order to determine the bounding conditions. The sequences that satisfied the selection criteria were analyzed to identify component failures (including component failures in support systems). Failure mechanisms were identified and estimates of failure frequencies were derived from generic failure rate data. Estimates of failure frequencies were also related to specific plant failure data when available.

Safety-significant control system failures identified by INEL and ORNL are described in Section 3.

PNL performed a probabilistic risk analysis on all significant failure sequences that were identified. The importance of these sequences was determined according to their expected contribution to risk.

For the more risk-significant failure sequences, plant modifications were evaluated and the potential risk reduction and cost for these modifications were estimated. A typical steamline configuration was analyzed (insofar as stress) to evaluate the dynamic effects of overfill events. These studies were performed by INEL through subcontracts with CREARE R&D Inc.

Evaluations were made to assess the generic applicability of the review. This review was conducted in two steps: (1) assessing whether the thermal-hydraulic characteristic of different plants (of the same vendor) were similar to the reference plants and (2) assessing whether control and safety systems of different plants (of the same vendor) are sufficiently similar.

2.4 Review Procedures

Similar methods and procedures were employed by INEL and ORNL to review the control systems. Differences were noted in the initiating mechanism for each type of transient evaluated, and in the number of control system failure combinations analyzed. These differences are attributed to the collective judgments made by the reviewers conducting the evaluations at each laboratory and the iterative process used to select the failure scenarios. These procedural differences are not significant.

2.4.1 Criteria Development

The following events for BWRs and PWRs were considered in identifying potentially significant control systems. These events were selected using the collective experience and judgment of the NRC staff and its consultants. Control systems whose failure could contribute to the listed events were identified by performing systems level failure mode and effects analyses (FMEAs) and were selected for detailed review as described in the following sections.

(1) BWR Events

(a) reactor coolant inventory increases and decreases
(b) reactor heat removal increase
(c) reactor vessel pressure increase
(d) reactor core positive reactivity increase
(e) reactor core recirculation flow increase and decrease

(2) PWR Events

(a) steam generator inventory increase and decrease
(b) increase and decrease in heat removal by the secondary system
(c) reactivity and power distribution anomalies
(d) decrease in reactor coolant system flow rate
(e) reactor coolant system inventory increase and decrease

Tables 2.1, 2.2, and 2.3 identify the screening criteria used by INEL and ORNL to identify potentially significant control systems.

2.4.2 Systems Level Failure Mode and Effects Analyses

A systems level FMEA was performed on all major plant systems for each reference plant design to identify systems and their failure modes that could potentially cause or contribute to the events listed above [Section 2.4.1(1) and (2)]. Systems that did not contribute to these events were deleted from further review. During this stage of review, non-safety-grade systems as well as safety-grade systems were addressed. A broad interpretation of the criteria (Tables 2.1, 2.2, and 2.3) was applied during the selection process to ensure that all systems that could contribute to the events of concern were identified, regardless of their relative effect. The effects of the failure of support systems (i.e., loss of air and loss of power supply, etc.), were also considered in this phase of the review.

2.4.3 Thermal-Hydraulic Transient Analyses

Thermal-hydraulic transient analyses were conducted using computer models developed for each of the reference plant designs.

Computer models included the nuclear steam supply systems, the balance of plant systems, the safety-grade reactor protection systems, and the major non-safety-grade control systems designed to control pressure, temperature, flow, and flux. The control logic necessary to automatically actuate the safety-grade and control-grade protection systems and/or components was included.

For the INEL analysis, RELAP 5/Mod 1.6 was used for both the GE and the W reference plant designs.

For the ORNL analysis, the computer model used for the B&W reference plant consisted of an analog model of the integrated control system coupled to a digital thermal-hydraulic model of the major reactor components and systems. This hybrid model (NRC, NUREG/CR-4449) utilized a number of different codes to model the various components and subsystems in the design. The codes most widely utilized were the RETRAN and RELAP codes.

For the CE reference plant design review, ORNL utilized the following plant models:

(1) a RETRAN model of Calvert Cliffs Nuclear Power Plant, Unit 1 [developed principally by CE for the Baltimore Gas and Electric Company and modified by ORNL (NRC, NUREG/CR-4758) to include the necessary control and balance of plant system designs], and

(2) a modular modeling system (MMS) computer code adapted to the Calvert Cliffs design.

The MMS model was developed as a backup in the event the RETRAN model might not be available. Subsequently, it was used for several transient simulations but was not needed for the design review.

Control system failures identified during the FMEA were represented in the thermal-hydraulic analysis. Single failures as well as multiple failures of systems such as loss of power to the control systems were evaluated to assess their effect on the transient behavior of the plant. It was not necessary in all cases to use the thermal-hydraulic model to evaluate the effects of every system failure identified by the FMEA. Engineering judgment limited the number and kind of transients that were performed. Selection of the type and number of system failures evaluated was an iterative process. That is, the selection of system failures was highly dependent on the results of previous analyses. In selecting credible single-failure and multiple-failure scenarios for analysis, engineering judgment prevailed. In some cases (more extensively in the reviews of the GE and the W designs), highly unlikely combinations of multiple failures were selected for analysis. These combinations were chosen to select system failure combinations that could have the most significant effect on the events of concern. If these selected multiple failures resulted in acceptable plant transients, many other (less severe) failure combinations could be eliminated from consideration. They were also selected to assess the effects of potential common mode failures of the more important systems.

If unlikely failure combinations resulted in significant plant transients, the failure modes were then analyzed to determine how credible these failure combinations were and to estimate the frequency of such failures.

Combinations of system failures under various normal plant conditions (i.e., startup, shutdown, and power operation) and accident conditions were analyzed. Failures that were considered for selecting worst-case or bounding transients included the following:

(1) single and multiple failure of safety-grade protection systems (evaluated only on GE and W designs)

    Some single failures in safety-grade protection systems could produce more severe transients than those caused by combined failures of various non-safety-grade control systems. In many cases, including the effects of safety-grade protection, failures bounded the effects of a number of non-safety-grade control system failure combinations and therefore minimized the number of non-safety-system failure combinations that needed to be analyzed by computer simulation.

(2) single failures of non-safety-grade systems

(3) multiple dependent failures of safety-grade protection systems and non-safety-grade systems resulting from a single event such as loss of a support system

(4) multiple independent system failures

Loss of ac and dc electric power supply systems and air systems were considered in the review. When multiple control system failures were identified that could occur as a result of a loss of a single electrical bus or a single air supply system or common sensing lines, they were analyzed. For certain systems, if it was not apparent from the available information whether or not they could fail simultaneously as a result of loss of power, multiple (dependent) failures were postulated. If these failures resulted in significant plant transients, the failure modes would then be analyzed to determine if these failures were credible.

For certain events, multiple independent failures of non-safety-grade systems (and safety-grade systems for the GE and the W review) were also evaluated. These analyses were performed in part to verify the dynamic plant response to failures that were assumed in the FSAR analysis (that is, a single failure of a safety-grade system concurrent with loss of a single non-safety-grade system) and in part to assess combinations of control system failures that might occur on other plants as a result of a common-cause failure resulting from unique design configurations. The number of control system failure combinations that were analyzed were minimized by selecting only those combinations that would have the greatest impact on plant parameters (i.e., flow, pressure, level, etc.). These combinations were judged to be the "worst case" scenarios. If these combinations resulted in acceptable plant transients, other (less severe) failure combinations could be eliminated from consideration.

2.4.4 Literature Search

The literature was searched to identify and evaluate transients or accidents initiated by failures related to control and instrument systems. Licensee event reports (LERs) and nuclear plant experience reports were reviewed to identify and select candidate scenarios for transient analysis. Control system failures from these reports were screened to identify those failures that could (a) adversely affect operator actions, (b) result in the actuation of protection systems, (c) cause technical specification safety limits to be exceeded, and (d) cause transients or accidents designated as moderate or infrequent events to occur more frequently than prescribed. Also, the LERs were used to assess if control system failures (shown by analysis not to be a problem on the reference plant) might be of concern on other plants. Data on control and instrument failures from 1969 through 1985 were reviewed by the laboratories. ORNL data were supplemented by additional data provided by the University of California at Los Angeles (UCLA) (Alter, 1983). UCLA staff visited seven plant sites, gathering operating experience and reviewing station records.

2.4.5 Failure Analyses of Significant Control System Failures

Failures that met the selection criteria (refer to Tables 2.1, 2.2, and 2.3) were considered to be safety significant. Analyses were performed to identify the credible failure mechanisms that could cause the events of concern. Probability estimates were also made for each identified failure mechanism, and for the resulting failure scenarios that could cause the events of concern. The results of these reviews are described in Section 3.

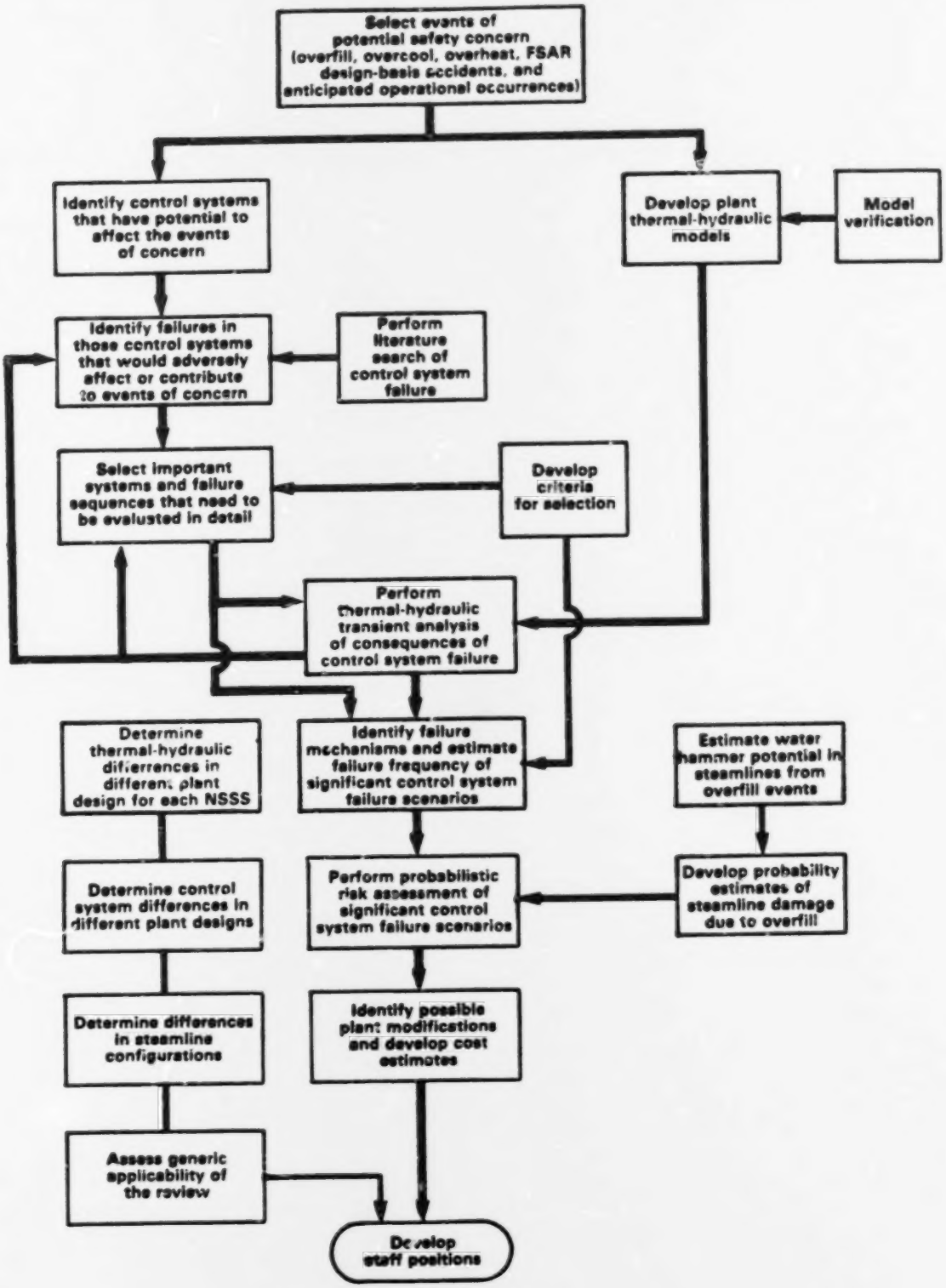
Select events of potential safety concern (overfill, overcool, overheat, FSAR design-basis accidents, and anticipated operational occurrences)
Identify control systems that have potential to affect the events of concern
Develop plant thermal-hydraulic models
Model verification
Identify failures in those control systems that would adversely affect or contribute to events of concern
Perform literature search of control system failure
Select important systems and failure sequences that need to be evaluated in detail
Develop criteria for selection
Perform thermal-hydraulic transient analysis of consequences of control system failure
Determine thermal-hydraulic differences in different plant design for each NSSS
Identify failure mechanisms and estimate failure frequency of significant control system failure scenarios
Estimate water hammer potential in steamlines from overfill events
Determine control system differences in different plant designs
Perform probabilistic risk assessment of significant control system failure scenarios
Develop probability estimates of steamline damage due to overfill
Determine differences in steamline configurations
Identify possible plant modifications and develop cost estimates
Assess generic applicability of the review
Develop staff positions

Figure 2.1 USI A-47 program overview

BEST COPY AVAILABLE

Table 2.1 Control system screening criteria used by INEL to identify potentially significant control system failures on the GE BWR reference plant design

(1) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in reactor coolant inventory to the point at which moisture enters the main steamlines, will be selected for a detailed review. For this study, the point of overfill is defined as that level which, if exceeded, could cause significant water to carry over into the main steamlines.

(2) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired decrease in reactor vessel inventory beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.

(3) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in heat removal beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review. System failures that could lead to cooldown rates in excess of 100°F in an hour were identified as potentially significant failures during the transient analysis phase of the review.

(4) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in reactor vessel pressure beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.

(5) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase or decrease in reactor core coolant flow beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.

(6) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in positive reactivity beyond the bounds of the Browns Ferry FSAR analysis, will be selected for a detailed review.

(7) Any control-grade system or component failures projected to cause transients identified as incidents of moderate frequency (anticipated operational occurrences) to occur more frequently than once a year, or failures which are projected to cause transients identified as infrequent incidents to occur more than once during the lifetime of a plant, or failures which are projected to cause limiting faults (design-basis accidents) will be selected for a detailed review.

(8) Any control-grade system or component failures that would adversely affect any assumed or anticipated operator action or operation of automatic protection systems during the course of a particular event, or that would result in frequent manual or automatic actuation of engineered safety features, including the reactor protection system, or that would result in exceeding any technical specification safety limit, will be selected for a detailed review.

Table 2.2 Control system screening criteria used by INEL to identify potentially significant control system failures on the W PWR reference plant design

(1) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in steam generator water level to the point at which moisture enters the main steamlines, will be selected for a detailed review. For this study, the point of overfill is defined as that level which, if exceeded, could cause significant water to carry over into the main steamlines.

(2) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase or decrease in reactor coolant inventory beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.

(3) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired decrease in reactor coolant water temperature beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review. System failures that could lead to cooldown rates in excess of 100°F in an hour were identified as potentially significant failures during the transient analysis phase of the review.

(4) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in nuclear system pressure beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.

(5) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired decrease in reactor core coolant flow beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.

(6) Any control-grade system or component failure, either initiating or aggravating, that results in an undesired increase in positive reactivity beyond the bounds of the H. B. Robinson FSAR analysis, will be selected for a detailed review.

(7) Any control-grade system or component failure, aggravating a steam generator tube rupture causing a release of radioactive material to the atmosphere greater than the FSAR analysis calculated, will be selected for a detailed review.

(8) Any control-grade system or component failures projected to cause transients identified as incidents of moderate frequency (anticipated operational occurrences) to occur more frequently than once a year, or failures which are projected to cause transients identified as infrequent incidents to occur more than once during the lifetime of a plant, or failures which are projected to cause limiting faults (design-basis accidents) will be selected for a detailed review.

(9) Any control-grade system or component failures that would adversely affect any assumed or anticipated operator action during the course of a particular event, or that would result in frequent manual or automatic actuation of engineered safety features, including the reactor protection system, or that would result in exceeding any technical specification safety limit, will be selected for a detailed review.

Table 2.3 Control system screening criteria used by ORNL to identify potentially significant control system failures on the B&W and CE PWR reference plant designs

(1)	Identify nuclear plant systems with potential to initiate or aggravate overfilling the steam generator. Such systems would be those whose failure or misoperation can introduce feedwater in amounts sufficient to fill the steam generator to the degree that water enters the steam lines.
(2)	Identify nuclear plant systems with the potential to initiate or aggravate overcooling the primary system. Such systems would be those whose failure or misoperation can lead to uncontrolled primary heat removal at rates greater than the rate of heat production to the extent where safety limits are challenged. System failures that lead to extended cooldown rates in excess of 100°F in an hour were identified as potentially significant failures during the transient analysis phase of the review.
(3)	Identify nuclear plant systems with potential to initiate or aggravate core damage through overheating.
(4)	Identify nuclear plant systems with potential to degrade the performance of safety systems.

3 RESULTS OF THE INEL AND ORNL STUDIES

3.1 Potentially Significant Control System Failure Scenarios

Using the methods and screening criteria described in Section 2, potentially significant control system failure scenarios were identified for each reference plant design. The results are summarized in the following sections.

3.1.1 GE BWR Plant

Three failure scenarios that could lead to reactor vessel overfill events were identified (NRC, NUREG/CR-4262, Vols. 1 & 2). Two of the three failure scenarios could also lead to overcool events during low-pressure startup or shutdown operation. All other failure scenarios that were identified were determined to be bounded by the plant FSAR analyses.

For these events, an assumption was made that no operator action would be initiated for the first 10 minutes following any postulated failure. This guideline applies to operator response to a specific failure regardless of the time at which the failure occurs during the course of an event.

The onset of overfill was predicted to occur very quickly (i.e., between 20 and 300 seconds into the event). The reactor vessel was assumed to overfill when moisture enters the main steamlines and is sustained. Moisture carryover was defined as a significant change in steam quality and was indicated by the steamline vapor void fraction and the downcomer water level. The transient analyses were terminated after the vapor void fraction in the steamline continued to decrease at a steady rate, indicating that more water was entrained in the steam. Transients that resulted in the downcomer fluid temperature decreasing at a steady rate greater than 100°F in an hour were defined as overcool transients. Table 3.1 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating the events of concern.

3.1.2 W 3-Loop PWR Plant

Eight failure scenarios were identified that could potentially lead to undesirable events (NRC, NUREG/CR-4326, Vols. 1 & 2). Two of these scenarios were identified as contributors to overfill events, two other scenarios contributed to overcool events, and two contributed to reactor coolant system overpressure events. The remaining two failure scenarios contributed to a radiation release during a steam generator tube rupture event, by causing greater break flow conditions than were assumed in the FSAR accident analysis.

Transient studies showed that the limiting mode of operation for one of the two identified overcool transients occurred during hot shutdown conditions. The two overpressure transients occurred during cold shutdown operation, and one of the overfill transients occurred during low-power operations. For the other failure scenarios, mid-range to full-power operation produced more rapid and severe transients.

For these events, an assumption was made that no operator action was initiated for the first 10 minutes following any postulated failure. This guideline applies to operator response to a specific failure regardless of the time at which the failure occurs during the course of the event.

Results of the thermal-hydraulic transient analysis indicated that:

(1) The onset of overfill (via the main feed water system) could occur very quickly (between 20 and 205 seconds).

(2) Plant cooldown transients reached cooldowns of 100°F within 125 to 230 seconds.

(3) Overpressure limits (10 CFR 50, Appendix G curves) can be exceeded in 15 to 162 seconds.

Table 3.2 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes the failure probabilities of control system failure sequences initiating the events of concern.

3.1.3 B&W PWR Plant

Three potentially safety-significant failure scenarios were identified (NRC, NUREG/CR-4047, -4449). One leads to a steam generator overfill event and two lead to a reactor core overheating event. The analysis indicates that the onset of overfill associated with main feedwater flow can occur very quickly (i.e., approximately 3 minutes) at power levels between 50% and 100% when both feedwater pumps are in operation. Overfill events associated with the auxiliary feedwater system and the startup feedwater system were predicted to occur at a much slower rate, so that the operator would be expected to have sufficient time to identify the event and terminate the flow before overfill conditions could occur. The onset of overfill was determined by a very low vapor void fraction fluid entering the steam generator downcomer and main steamlines. This guideline was similar to that discussed in Section 3.1.1 for the BWR review.

For the overheat events, it was predicted that the core could be severely damaged if the operator did not take proper corrective action within 30 to 60 minutes.

Other control system failure scenarios were identified in NUREG/CR-4047 and NUREG/CR-4449, but were determined to be either bounded by transients or accidents analyzed in the FSAR, or it was determined that the operator would have sufficient time to terminate the event before it became a safety-significant event; therefore they are not discussed here. Table 3.3 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating or contributing to the events of concern.

3.1.4 CE PWR Plant

Four potentially safety-significant failure scenarios were identified (NRC, NUREG/CR-4265). Two lead to overfilling the steam generator vessel via the

main feedwater system; one leads to overheating the reactor core; and one overcooling event could lead to a possible pressurized thermal shock event in a plant with a vulnerable pressure vessel. Two categories of such overfill events were investigated: rapid and slow. Slow overfeed transients occur via the feedwater bypass valves after the main feedwater regulating valves are closed and were not considered safety significant because of the long time it took to overfill. Overfill with main feedwater systems was predicted to occur very quickly (that is, onset of overfill could occur in 2 minutes). Onset of overfill was assumed when low-quality steam entered the main steamlines. This guideline is similar to that discussed in Section 3.1.1 for the BWR review. For the other two failure scenarios, the analysis indicated that for a very narrow range of break sizes of small-break LOCA (SBLOCA) events, overheating of the core or possible pressurized thermal shock can occur if the operator fails to take the plant to safe-shutdown conditions. Other failure scenarios were identified in NUREG/CR-4265 but were determined to be bounded by the events analyzed in the FSAR accident analysis, or it was determined that the operator would have sufficient time to terminate the event. Therefore they are not discussed here.

Table 3.4 summarizes the failure scenarios and the failure mechanisms that were identified as safety significant, and summarizes failure probabilities of control system failure sequences initiating or contributing to events of concern.

3.2 Literature Search

Licensee event reports (LERs) and nuclear plant experience reports were reviewed to identify control system failures that could (1) adversely affect operator actions, (2) result in the actuation of protection systems, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents designated as moderate or infrequent events to occur more frequently than described. Data on control and instrument failures from 1969 through early 1985 were reviewed. The following sections summarize that review and the conclusions.

3.2.1 GE BWR Plants

The literature review for BWR plants evaluated all reported control system failure events for the Browns Ferry Nuclear Power Station, Units 1, 2, and 3, during a 3-year period (1980 through 1982). This review was expanded to include all other BWR plants for the same period. The data were further expanded to include potentially significant events occurring as early as 1970 (NRC, NUREG/CR-4262, Vols. 1 & 2).

Review of the operating experience did not identify any control system failures that satisfied the above criteria.

Three reactor overfill events did occur in the early 1970s. Two occurred at Dresden Nuclear Power Station, Units 2 and 3, and one at Nine Mile Point Nuclear Station, Unit 1. At the time of these events, the design did not provide a high reactor vessel level feedwater trip system. A trip system was later incorporated.

Four overcooling events were also identified [Edwin I. Hatch Nuclear Plant, Unit 2 (1978); Brunswick Steam Electric Plant, Unit 1 (1977); Peach Bottom

Atomic Power Station, Unit 3 (1979); and Cooper Nuclear Station (1980)]. These events were used as precursors to the transients evaluated in the plant model.

3.2.2 W PWR Plants

A similar review of the W PWR plants was conducted for the same 3-year period i.e, 1980 to 1982 (NRC, NUREG/CR-4326, Vols. 1 & 2). The review included the reference plant and five other W PWR plants. The review did not identify any control system failures that satisfied the criteria stated above.

3.2.3 B&W PWR Plants

A review of the operating experience was conducted for the reference plant and all other B&W PWR plants (NPC, NUREG/CR-4047). The period ranged from January 1975 through early 1985. On the basis of this review, there were no abnormal events at the reference plant that led to potentially severe accidents or unsafe conditions. One steam generator overfill event occurred at Oconee Nuclear Station, Unit 3, in 1981.

The operating history data on other B&W PWR plants revealed the following:

(1) Two steam generator overfill events occurred at Rancho Seco Nuclear Generating Station, Unit 1 (March 1978 and December 1985).

(2) Operator errors could cause violations of technical specifications.

(3) Inadvertent malfunctions occurred infrequently.

(4) Unnecessary scrams that challenge the protection system occur. B&W PWR plants have a lower-than-average industry record for the number of scrams (i.e., three per year)

3.2.4 CE PWR Plants

A review similar to the B&W review was conducted for CE PWR plants (NRC, NUREG/CR-4449).

A number of steam generator overfeed events were identified; none progressed to an overfill condition. In all cases, the overfeed events were terminated by the control system or by operator action. Maintenance and testing problems resulted in the most frequent challenges to the protection systems. The review did not identify any control system failures that satisfied the criteria stated in Tables 2.1, 2.2, and 2.3.

Table 3.1 Potentially significant failure scenarios in a representative GE BWR

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event #1	Failure in the feedwater control system can cause an increase in feedwater flow and disable the feedwater trip system, and the operator fails to trip the feedwater pumps. Condition for Operation: 67% full load operation	A leak or rupture of the primary sensing line common to two of the three reactor vessel water level sensors, causing false low-level signals Common cause failure (e.g., maintenance error) of two of the three reactor vessel level sensors (or sensor circuitry), causing false low-level signals Independent failures of two of the three level sensors (or sensor circuitry) causing false low-level signals. A failure in the control circuit that regulates the feedwater pump speed and a second failure of two of the three high-level trips	3.4E-3*
Overfill event #2**	Control system failure can cause an increase in the condensate flow and the operator fails to terminate condensate flow. Condition for Operation: Low-pressure startup or reactor shutdown operation.	A single control system failure can cause any one of the three motor operated feedwater pump discharge valves to open, resulting in full condensate flow A single failure of a startup feedwater low-pressure bypass valve (failing open) can cause an increase in the condensate flow rate A single failure of a condenser bypass valve (failing closed) can cause an increase in the condensate flow rate	2.5E-5†

See footnotes at end of table.

Table 3.1 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event #3**	Failure in the protection system which results in inadvertent low-pressure coolant injection (LPCI) or core spray injection (CSI) and the operator fails to terminate flow. Condition for Operation: Low-pressure startup or reactor shutdown operation	Failure in a one-of-two-taken-twice reactor low water level logic circuit Failure in one of the two high drywell pressure logic circuits Common cause failure of two drywell pressure switches (failing closed) Common cause failure of two reactor vessel low water level switches (failing closed) Two independent failures of drywell pressure switches or two independent low reactor water level switches (failing closed)	1.6E-3††

*Includes probability estimate (0.52/demand) that the operator fails to trip the feedwater in time to prevent overfill following a rapid overfeed transient.

**This event can also cause an overcool transient.

†Includes probability estimate (0.3/demand) that the operator fails to trip the condensate flow to prevent overfill.

††Includes probability estimate (0.4/demand) that the operator fails to trip the LPCIs or CSIs.

Table 3.2 Potentially significant failure scenarios in a representative W PWR

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event #1	A single control system failure can lead to excessive feedwater flow (e.g., overfeed). When the feedwater flow is automatically terminated by the high steam generator level trip system, the auxiliary feedwater system (which is automatically initiated when the main feedwater pumps are tripped) can cause a steam generator overfill condition if the operator does not take proper action to mitigate the transient. Condition for Operation: Very-low-power operation (i.e., 5% power).	A false steam generator low-level signal to the feedwater controller could cause overfeed of a steam generator A leak or rupture in the primary sensing line of the controlling steam generator level instrument could cause overfill A single failure could cause the feedwater regulating valve to open and cause an excessive overfeed transient A failure in the steam genearator water level controller circuitry could cause a steam generator overfeed transient	1E-4*
Overfill event #2	A control system failure causing an increase in main feedwater flow and a second failure of a high steam generator water level trip system could cause an overfill event if the operator fails to terminate flow. Condition for Operation: 67% full-power operation	A failure in the controlling steam generator level instrument (causing it to indicate low) and a concurrent (or subsequent) second failure of another level channel (sticking or failing as is) A leak or rupture in the primary sensing line of the controlling steam generator level instrument and a second failure of another level channel (sticking or failing as is) A failure in the main feedwater valve (causing it to open) and a failure of two of the three steam generator level instruments (fail in the mid-range position)	3E-8**

See footnotes at end of table.

Table 3.2 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event #2 (cont'd)		A failure of a steam generator level controller and a failure of two of the three steam generator water level instruments failing to respond to a high-level condition	
		The controlling steam generator level instrument fails low and the high steam generator water level trip logic circuitry fails to trip the feedwater pumps	
		A leak or rupture of the primary sensing line of the controlling level instrument (causing the sensor to read low) and a failure of the high-level trip logic circuit	
		A failure of a feedwater valve (in the open position) and a failure of the high-level trip logic circuitry	
		Failure of the steam generator water level controller and a failure of the high-level trip logic circuitry	
Overcool event #1	A failure that results in an inadvertent steam dump operation with the reactor at power (all steam dump valves fail open and the operator fails to initiate block valve). Condition for Operation: 102% full-power operation (this failure scenario requires that the reactor trips during the early stage of the transient)	The T_{ave} temperature instrument fails high and a second failure in the steam dump valve arming circuit	1.4E-8†
		A single failure in the temperature controller and a second failure in the steam dump valve arming circuit	

Table 3.2 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overcool event #2	Control system failure that results in inadvertent opening of steamline relief valves. Condition for Operation: Hot shutdown (T_{ave} less than 547°F)	Single failure in the steam dump controller that sends a signal to one or more steam dump valves A single failure in a steam dump valve that results in opening of the valve A single failure in the steam dump controller that sends an open signal to one or more PORV (atmospheric dump valves) A steamline PORV control circuit (or switch) fails	1E-3†
Overpressure event #1	A failure that results in a loss of letdown flow and a loss of pressure relief (both PORVs) and the operator fails to terminate the event. Condition for Operation: Cold shutdown	A loss of power that feeds both the letdown valve and one of the PORVs so that the pressurizer letdown valve goes to its closed position capability and renders the PORV inoperable and a second active failure of the other PORV Independent failure of a letdown valve in the closed position and failure to open both PORVs	2E-8††
Overpressure event #2	A failure that results in inadvertent safety injection initiation when the reactor is being heated from cold shutdown. (During this operation both pressurizer PORV setpoints are shifted from the "low temperature" setpoint to the "normal" setpoint. If there is a failure causing inadvertent operation	A single failure in the logic circuit that results in the actuation of the safeguards sequence Independent failures that would initiate high-pressure safety injection and open the accumulator isolation valves	4E-5††

See footnotes at end of table.

Table 3.2 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Over-pressure event #2 (Cont'd)	of safety injection, overpressure conditions can occur if the operator fails to terminate the event). Condition for Operation: Heating up from cold shutdown	A single failure in one of the two safety injection actuation pushbuttons (that actuates the safeguards sequence)	
SGTR event #1	Failure that results in opening one of the steamline relief valves concurrent with a steam generator tube rupture in the affected steam generator. Condition for Operation: 102% power operation with one steam generator tube ruptured (adjacent to the cold-leg tube-sheet) and a simultaneous loss of off-site power	A failure of a component in the steam-line PORV control circuit that causes the valve to open and remain open) A mechanical failure of a steamline PORV (i.e., atmospheric dump valve) that causes the valve to stick open A failure of a component in the steam dump controller causes a steamline PORV to open and remain open A mechanical failure of a safety valve causes it to stick open	2E-3 (7E-6 with an SGTR event)
SGTR event #2	Failure that results in opening of steamline safety valves (SRVs) or steam-line relief valves (PORVs) and a high feedwater rate concurrent with a rup-ture of a steam generator tube. Condition for Operation: 102% power with one steam generator tube rupture (adjacent to the cold-leg tubesheet)	For PORV and SRV failure mechanisms, refer to steam generator tube rupture event #1 above For feedwater overfeed events, the following failure mechanisms were considered: · A failure of a steam generator level instrument controlling the feedwater flow	3E-3 (1E-5 with an SGTR event)

See footnotes at end of table.

Table 3.2 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
SGTR event #2 (Cont'd)		• A leak or rupture of the sensing line of the level instrument controlling the feedwater flow	
		• Inadvertent opening of the feedwater control valve	
		• A circuit failure of the steam generator water level controller	

*Includes probability estimate (0.1/demand) that the operator fails to terminate the auxiliary feedwater system to prevent overfill.

**Includes probability estimate (0.5/demand) that the operator fails to terminate the flow.

†Includes probability estimate (0.05/demand) that the operator fails to initiate the block valve.

††Includes probability estimate (0.1/demand) that the operator fails to terminate the event.

Table 3.3 Potentially significant failure scenarios in a representative B&W PWR

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event	Failure in the main feedwater control system (or valves) that could result in overfeeding one of the two steam generators and a concurrent (possibly long-present but undetected) failure of the main feedwater pump trip system which terminates feedwater flow on high steam generator level and a failure of the operator to detect and manually trip the main feedwater pumps or isolate the feedwater flow. Condition for Operation: Normal power operations	Failures that can cause main feedwater pump trip system to fail are: · Either of two high steam generator (operate range) level transmitters failing low · Either of two steam generator level function generator modules failing · Either of two multiplications modules failing. · Either of two signal monitors failing · Feedwater pump trip relay (FTPX) failure · Feedwater pump trip solenoid valve failures · Feedwater pump turbine inlet intercept valve failures Failures that can cause main feedwater overfeed are: · Main feedwater control valves fail open or control valve signal fails demanding valve to open · Miscellaneous failures of control modules associated with the feedwater control system	6E-3*

See footnotes at end of table

Table 3.3 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overheat event #1	A loss of electric power to the integrated control system branch circuits "H" or "H1" when the control system is operating in the automatic mode would result in control stations for different control systems transferring to a manual mode of operation. This transfer could occur without upsetting plant operation. Power could be restored before any plant perturbations could occur. If, however, plant perturbations resulted in a reactor trip, feedwater overfeed conditions could occur if the operator does not manually throttle the feedwater flow. The feedwater pumps would eventually trip on high steam generator level if the feedwater flow was allowed to continue and safe-shutdown operations would be initiated. If, however, the operator takes action early in the transient in throttling the feedwater to prevent overfeed, but subsequentially does not restore the necessary flow to the steam generator or initiate high-pressure injection (HPI), severe reactor core overheating can occur. Condition for Operation: Normal operating range	A loss of "auto" power to integrated control system branch circuit "H" or "H1".	1.4E-6**

See footnotes at end of table.

Table 3.3 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overheat event #2	A failure of the "hand" power to the feedwater control system would result in the main feedwater pump run back to minimum speed. If the feed pumps were not tripped but allowed to operate at minimum speed, the steam generator water level would eventually be depleted. Unless the operator manually initiates the auxiliary feedwater system or restores the main feedwater flow, the steam generator would boil dry and steam generator cooling would be lost. The operator has about 30 minutes to reestablish the main or auxiliary feedwater flow. After 30 minutes, establishing feedwater flow would not be effective to establish the necessary steam generator cooling. The high-pressure injection pumps would provide the necessary long-term core cooling if the operator manually initiates this system within 60 minutes. Condition for Operation: Normal power operations	Loss of "hand" power to the integrated control system branch circuits (HX or H1X)	9E-6†

*Includes probability estimate (0.7/demand) that the operator fails to trip the feedwater in time to prevent overfill following a rapid overfeed transient.

**Includes probability estimate (0.03/demand) that the operator fails to reinstate main feedwater or initiate emergency feedwater within 30 minutes, and includes a probability estimate of 0.01/demand that the operator fails to initiate high-pressure injection within 60 minutes.

†Includes probability estimate (0.3/demand) that the operator fails to reinstate main feedwater or initiate emergency feedwater within 30 minutes, and includes a probability estimate of 0.01/demand that the operator fails to initiate high-pressure injection within 60 minutes.

Table 3.4 Potentially significant failure scenarios in a representative CE PWR

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overfill event #1	A single failure which causes the main feedwater regulating valve to fail in the "as is" or in the fully open position and the operator fails to terminate the overfeed event. Condition for Operation: Transient conditions following a reactor trip	The following failures can cause the main feedwater regulatory valves to fail: · Loss of electrical bus (1Y09) · Air solenoid valve controlling air to the feedwater regulatory valve fails closed · Mechanical failure of the main feedwater regulating valve · Failure in the hand/auto station to the regulating valve · Failure of the electrical to pneumatic convertor to the main feedwater regulating valve	9E-3*
Overfill event #2	Given an overfeed condition, if the turbine trip signal to the feedwater regulating circuit fails and the operator fails to terminate the feedwater flow, a system generator overfill event can occur (multiple failures would be required). Condition for Operation: Normal power operation	An overfeed condition can occur if the feedwater demand signal fails high and the following failures occur to cause the turbine trip signal to fail to close the regulating valves: · Logic circuit failure · Relay failure · Cable failure	4E-4*

See footnotes at end of table.

Table 3.4 (Continued)

Frequency event	Failure scenario	Failure mechanism	Estimated events/year
Overheat event	Given a specifically sized small-break loss-of-coolant accident (LOCA), a failure to initiate reactor coolant system cooldown via the steam generator, and/or depressurize the reactor via the pressurizer power-operated relief valve (PORV) or the auxiliary spray system can potentially cause core uncovery. Condition for Operation: Shutdown after a small-break LOCA	A failure to initiate or maintain reactor coolant system cooldown can be caused by atmospheric dump valves (ADVs) and/or the turbine bypass valves (TBVs) failing to open on demand, or closing indirectly as a result of a safety injection actuation signal and an operator error A failure of the instrument air system or a loss of power to bus Y09 can prevent the ADVs and TBVs from opening (these have much lower probabilities than the mechanism above) A failure to depressurize the reactor coolant system can result from the lack of procedural instructions to initiate this mode under saturated RCS conditions	9E-6**
Overcool event	Given a small-break LOCA and reactor coolant system cooldown is initiated, if the operator fails to open either pressurizer PORV or initiate auxiliary spray, a pressurized thermal shock could result in damage to a vulnerable pressure vessel. Condition for Operation: Shutdown after a small-break LOCA	Operator error or a failure of the pressurizer PORVs or auxiliary spray system	1.5E-4†

See footnotes on next page.

Table 3.4 (Continued)

*Includes 0.1/demand probability that the operator fails to manually trip the main feedwater pumps in time to prevent overfill.

**Includes multiple operator failure probabilities (that is, failure to initiate reactor coolant system (RCS) cooldown via the steam generator (0.01/demand) and failure to depressurize the RCS via pressurizer PORVs or auxiliary spray system (0.5/demand).

†Includes 0.01/demand probability that the operator fails to open the pressurizer PORV when indicated. It does not include the conditional probability of vessel failure due to pressurized thermal shock (PTS) conditions.

4 GENERIC APPLICABILITY

Reference plants were selected on the basis of (1) the quality and quantity of design information available to conduct a review and (2) the belief that any weaknesses in control system designs were more likely to be identified in older plants.

A number of control system failures were identified at the reference plants that had the potential for causing undesirable events. To determine if the results obtained for the reference plants were applicable to other plants (for the same vendor), similarities in the thermal-hydraulic parameters and similarities in control systems of other plants were evaluated. This evaluation of control systems (similarity review) of other plants focused primarily on those design characteristics identified as contributing to the events of concern. Sensitivity studies were selectively performed to evaluate if the differences were significant. The significant transients analyzed for the reference plants were also evaluated to determine (1) if similar transients could occur in other plants and (2) if the transients analyzed for the reference plant represented a more severe or bounding transient.

Results of the review of the reference plants were considered generically applicable to other plants of the same vendor if:

(1) Major fluid systems of other plants were functionally similar to the reference plant.

(2) Power-to-volume ratios and various volume-to-flow ratios of other plants were similar to the reference plant.

(3) Thermal-hydraulic transients analyzed at the reference plant were similar or would bound transients on other plants of the same class.

(4) Control systems at other plants were sufficiently similar to control systems at the reference plant that any differences in the design were not significant enough to substantially alter the events of concern.

(5) Reactor protection systems (that is, the reactor trip systems and the engineered safety features systems) at other plants are functionally similar to the systems of the reference plants so that any differences in the design of the reactor protection system were not significant enough to substantially alter the events of concern.

A large number of single and multiple control system failures were analyzed on the reference plants. It was not necessary or practical to evaluate all possible control system failure combinations that could occur in any one plant. Engineering judgment and the FMEA conducted on each plant were used to limit the number and kind of transient analyses performed. Selection of the type and number of system failures evaluated for the plant model was an iterative process highly dependent on the knowledge gained from responses to the failure sequences

simulated in previous analyses. In some cases, highly unlikely combinations of multiple failures were evaluated to assess worst-case or bounding scenarios. On the basis of the combinations and number of control system failures analyzed, it became apparent that as long as the protection systems were not compromised and performed their intended design functions, the events (except those noted below) induced by control failures were satisfactorily mitigated. On the basis of the number of credible and unlikely failures evaluated, the staff concluded that other control system failures that could occur on the reference plant (but have not been analyzed in this review) would also be mitigated by the protection systems. Since the designs of the reactor protection systems of other plants (of the same vendor) are functionally similar to the reference plant design, the same degree of protection to mitigate multiple control systems failures is provided in other plants.

It should be noted that a few plant designs vary significantly from the reference plant designs. These plants incorporate unique design features in major fluid systems and/or instrumentation and control systems, power systems, or reactor protection systems which have not been evaluated in detail. For BWRs these plants are: Oyster Creek Nuclear Power Plant, Unit 1; Big Rock Point Nuclear Plant; Nine Mile Point Nuclear Station, Unit 1; La Crosse Nuclear Generating Station; Millstone Nuclear Power Station, Unit 1; and Dresden Nuclear Power Station, Units 2 and 3. For the W PWRs, the plants are: Yankee Rowe Nuclear Power Station, Haddam Neck Plant, and San Onofre Nuclear Generating Station, Unit 1. For CE PWRs, the plants are: Arkansas Nuclear One, Unit 2; San Onofre Nuclear Generating Station, Units 2 and 3; Maine Yankee Atomic Power Plant; and Palo Verde Nuclear Generating Station, Units 1, 2, and 3. For B&W PWRs, the plants are Arkansas Nuclear One, Unit 1; Crystal River Nuclear Plant; Rancho Seco Nuclear Generating Station, Unit 1; and Davis-Besse Nuclear Power Station, Unit 1, The major differences in these designs and their effects on the significant events are discussed below. Most of the events identified during the USI A-47 review were found to be generically applicable to most other reactors of the same class. Some events, however, were determined to be applicable only to the reference plant.

The following discussions assess the generic applicability of the events determined to be safety significant during the review. Design features of other plants that could potentially modify failure scenarios or transients analyzed in this review are described and the criteria used to assess generic applicability are identified. This assessment is based on fundamental engineering principles, the generic evaluations conducted by ORNL and INEL (see reference NRC reports and Letter Report), and staff judgment.

4.1 GE BWR Plants

Several control system failures that could contribute to reactor vessel overfill and reactor overcool events were identified as potentially safety significant. All other control system failures that were evaluated were determined to be bounded by the FSAR analyses. The failure mechanisms contributing to these events are identified in Table 3.1. Major contributors to events that occur during power operation were multiple control system failures that initiated overfeed transients and failed the automatic feedwater pump trip system. Major contributors to events that occur during startup or shutdown operation were single and multiple failures that initiated vessel overfeed.

The following discussions summarize the design features of other plants and assess the generic applicability of the major events identified for the reference plant.

4.1.1 Overfill Events at Power Resulting From Failures in the Reactor Vessel High-Level Feedwater Trip System

(1) Control Systems Differences

Review of the plant-specific safety analysis reports (SARs) and the docket files identified variations in the reactor vessel high-level feedwater trip systems which terminate reactor vessel overfill events in BWRs during power operation.

Most operating BWR plants provide commercial, non-safety-grade reactor vessel overfill protection identical to the reference plant; that is, a 2-out-of-3, high-level trip system with separate and independent electrical power supplies for each level sensor. Several plants however have overfill protection designs with less independence and reliability. These designs vary from a 1-out-of-1 or a 1-out-of-2, to a 2-out-of-2 reactor high-level feedwater pump trip. On some plants, logic separation and electrical power independence could not be verified. More recent designs provide improved flexibility and redundancy by including a four-level sensor logic system, that is, a 1-out-of-2 taken twice. Three plants (Big Rock Point, LaCrosse, and Oyster Creek) have no automatic isolation of feedwater on a high reactor vessel water level signal and rely solely on the operator to mitigate an overfeed event.

The relative benefits of the different high-level trip logic provisions were evaluated using the reference plant as a model. The risk reduction associated with the different trip systems was estimated (NUREG/CR-4387).

Safety benefits gained by providing additional reactor vessel level redundancy and independence to some existing feedwater trip systems are not significant. The estimated reduction in frequency of overfill events between plants that have some sort of automatic reactor vessel high-level feedwater trip system was not significant. For plants with no automatic feedwater trip system, the overfill frequency was estimated to be about 15 times more likely than for plants with automatic feedwater trip systems. In actual practice, the three BWR plants with no trip system have demonstrated better reliability because of the operator's role in controlling feedwater. Results and conclusions of analyses of the reference plant apply to other BWR plants if they meet the following criteria with respect to control system design.

(a) The plant must have an automatic reactor vessel high-water-level feedwater trip system.

(b) The trip system must be operable during power operation or administrative procedures must be implemented to ensure that manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is not operable.

(2) Thermal-Hydraulic Differences

Most BWR plant systems that could contribute to reactor vessel overfeed and vessel overfill events are functionally similar. Although variations in the design exist in some plants, such as the number, type, and capacity of valves or pumps and the size of reactor vessels, these variations are not significant when the overall size of the plant is considered. Major systems are designed with roughly similar proportions so that the time to overfill on other BWR plants is expected to be very similar to or bounded by the time predicted for the reference plant. Several BWR plants identified above (p. 4-2) incorporate designs that differ from the reference plant design. These differences include: (1) different recirculation flow systems, (2) use of isolation condensers, (3) different power supply designs, and (4) use of different reactor vessel capacities.

These design differences (except for vessel size) would not change the results of the overfill transients analyzed for the reference plant. Although reactor vessel capacity (i.e., size) can affect plant response for overfill events, the feedwater flow to reactor vessel volume ratio for these plants is smaller than the ratio for the reference plant so that the overfill transients on plants with larger reactor vessel volumes (like La Crosse) are expected to be slower than predicted for the reference plant.

The following criterion was used to assess the generic applicability of this overfill event at other plants: Power to flow, power to volume, and reactor feedwater flow to reactor vessel volume ratios for other plants should be similar to the ratios for the reference plant. If the ratios vary, they should vary in the direction to cause the overfill transients to occur more slowly.

Plants with thermal-hydraulic characteristics that satisfied this criterion were determined to be similar to the reference plant.

(3) Conclusions

(a) Most BWR plants provide automatic feedwater pump trip systems on high reactor vessel level. (Only three plants do not have automatic feedwater pump trip on high reactor vessel level).

(b) Variations in the design of the control system for automatic overfill protection exist in other BWRs. For plants with automatic overfill protection systems, variations in the design do not significantly modify expected failure estimates to reduce the frequency of overfill events that could result from control system failures.

(c) For plants with no automatic overfill protection, overfill events are estimated to be 15 times more likely than for plants with automatic overfill protection. Operator action can significantly reduce this estimate.

(d) Power to flow, power to volume, and reactor feedwater flow to reactor vessel volume ratios for other BWR plants are sufficiently similar to these ratios for the reference plant that the analysis conducted on the reference plant is considered a bounding analysis and is generically applicable to other BWR plants.

4.1.2 Overfill and Overcool Events During Low-Pressure Startup and Shutdown Operations

(1) Control System Differences

Various failures in the condensate system and in the low-pressure coolant injection (LPCI) and core spray (CS) systems were identified that could cause reactor vessel overfeed events during low pressure startup and shutdown operations.

Most BWR plants provide LPCI, CS, and condensate systems similar to systems in the reference plant design. Although variations in some control system designs exist, all plants rely on the operator to terminate flow from these systems once they are initiated.

(2) Thermal-Hydraulic Differences

Several plants provide fluid system designs that are different from the reference plant design. These differences are discussed in Section 4.1.1.

The differences in the major fluid systems in these plants (except for reactor vessel size) do not affect the overfill transients analyzed for the reference plant. For plants with larger reactor vessels, because the ratio of condensate flow and/or emergency core cooling system (ECCS) flow to the reactor vessel volume is smaller than these ratios for the reference plant, overfill transients for these plants are expected to be slower and less severe than the transients predicted for the reference plant.

The following criteria were used to assess the generic applicability of this event on other plants:

(a) Power to flow, power to volume, and condensate flow or low-pressure ECCS flow to reactor volume should be similar to the values for the reference plant.

(b) The fill rate of the condensate system or the ECCS is less than or about equal to the reference plant flow rates.

(c) Administrative procedures are implemented to help ensure that manual trip can be accomplished to terminate condensate or ECCS flow in time to prevent overfill.

Plants that had thermal-hydraulic characteristics and administrative procedures satisfying these criteria were determined to be similar to the reference plant.

The risk associated with control failures that could lead to overfill events (estimated for the reference plant) was small. Because the variations in control system design for other plants were not significant enough to substantially increase these estimates, sensitivity studies of control systems contributing to this event at other BWR plants were not performed.

(3) Conclusion

Power to flow, power to volume, and condensate flow or low-pressure ECCS flow to reactor volume ratios at other BWR plants are similar enough to the reference

plant so that the analysis conducted on the reference plant is considered a bounding analysis and is generically applicable to other BWRs.

4.2 W PWR Plants

The review of a W PWR plant identified several control system failures that could contribute to steam generator overfill, reactor vessel overcool, and reactor overpressure events. Several failures were also identified that could contribute to undesirable release [i.e., releases in excess of those calculated in the FSAR analysis for steam generator tube rupture (SGTR)] of radioactivity during an SGTR. All other control system failures that were evaluated were determined to be bounded by the FSAR analysis. The failure mechanisms that contribute to these events are identified in Table 3.2. Overfill events could be caused by either sustained operation of the auxiliary feedwater system or the main feedwater system. Overcool events could be caused by failures in the steam dump control systems (i.e., steamline atmospheric dump valves or condenser steam dump system). Overpressure events could be caused by failures in the pressurizer power-operated relief valve (PORV) control system, failures of the letdown valves, and failures in the ECCS circuitry. Failures in the steamline pressure relief control systems could also contribute to excessive release of radioactivity during an SGTR.

The following discussions summarize the generic applicability of other W PWR plants to the major events identified in the reference plant.

4.2.1 Overfill Events Resulting From a Sustained Operation of the Auxiliary Feedwater Flow

(1) Control Systems Differences

On all W PWR designs, auxiliary feedwater (AFW) flow is automatically initiated when the main feedwater pumps are tripped. There are no automatic interlocks to terminate AFW flow when the level reaches a high steam generator level (except for Virgil C. Summer Nuclear Station, Unit 1). An overfill event similar to the reference plant event can occur unless the operator manually terminates the AFW flow. Analysis performed on the reference plant predicts onset of overfill occurring so rapidly that quick operator response is needed to terminate the AFW flow.

Results and conclusions of analysis performed on the reference plant apply to other W PWR plants if they do not meet the following criteria with respect to control system design.

(a) Automatic reduction of the AFW flow on steam generator high level is provided, or

(b) Administrative procedures are implemented to give reasonable assurance that manual throttling of the AFW can be accomplished in time to prevent overfill.

If other W PWR plants meet the above criteria, the analyzed failure modes would be less severe than for the reference plant and should not result in a steam generator overfill.

(2) Thermal-Hydraulic Differences

Variations exist in the design of the AFW systems in other W PWR plants that would change the time to overfill.

New 4-loop designs and some 3-loop designs have devices (orifices or throttling valves) installed in the AFW lines. These devices restrict the flow into the steam generators so that a less severe overfeed transient would result than analyzed for the reference plant. In addition, most 4-loop designs have split AFW headers, so only 50% of total AFW could flow into the faulted steam generator instead of 100% flow for the 3-loop reference plant design.

The following criterion was used to assess the generic applicability of this event on other plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than these ratios for the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

Some W PWR plants identified above incorporate designs that are different from the reference plant. These design differences include: (a) large cooling capacity of the reactor coolant system so that the ratio of the steam generator volume to the main or auxiliary feedwater flow is significantly greater than the reference plant design; (b) the use of charging pumps which have a higher pressure capability than the reference plant design; and (c) the use of charging pumps which have no main steam isolation valves. These design differences would not change the results of the overfill events analyzed for the reference plant with the exception of plants with larger reactor vessel volumes. For those plants, less severe overfill events are expected.

Although other differences, such as operator training and procedures and the design of the level indication system and alarms available to the operator, will alter the operator response time to address an overfeed event, the review did not identify any plants that would have more severe overfill transients.

(3) Conclusion

(a) Overfill events via the AFW system can occur at other W PWR plants under similar conditions analyzed in the reference plant (except for the Virgil C. Summer plant which has automatic termination of AFW).

(b) The overfill transients via the AFW system at other W PWR plants are determined to be equal to or less severe than those analyzed for the reference plant (except for the Virgil C. Summer plant which has automatic termination of AFW).

(c) Steam generator volume to main feedwater flow rate and steam generator volume to AFW flow rate ratios at other W PWR plants are so similar to reference plant ratios that the overfill analysis conducted at the reference plant is considered a bounding analysis applicable to other W PWR plants. Although several plants provide different designs, so that some

of the thermal-hydraulic characteristics mentioned above are different from the reference plant, the differences are such that the transients would be equivalent to or less severe than the results of the overfill events analyzed for the reference plant.

4.2.2 Overfill Events Resulting From Failures in the Steam Generator, High-Level, Feedwater, Trip System

(1) Control System Differences

All of the overfill protection system designs at W PWR plants (except for three very early plant designs, i.e., Haddam Neck, Yankee Rowe, and San Onofre 1) have either a 2-out-of-3 or a 2-out-of-4 steam generator, high-water-level, trip system to terminate the feedwater flow during a feedwater overfeed event. These systems are redundant and designed to satisfy safety requirements. The newer designs incorporate a more flexible and redundant 2-out-of-4 system that provides additional improvements for testing and fully satisfies all the prescribed safety requirements of IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." San Onofre 1 and Yankee Rowe plants do not have automatic overfill protection. The Haddam Neck plant provides an overfill protection system consisting of a safety-grade, 1-out-of-2, steam generator high-water-level interlock which automatically shuts the main feedwater control valves to the steam generator. Results and conclusions of the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system design:

(a) The plant must have an automatic steam generator, high-water-level, feedwater, trip system similar to or better than the reference plant design has.

(b) The trip system must be operable during power operation or administrative procedures must be implemented to provide reasonable assurance that a manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is inoperable.

(2) Thermal-Hydraulic Differences

The following criterion was used to assess the generic applicability of this event to other W PWR plants: Steam generator volume to main feedwater flow rate ratio should be similar to or greater than that of the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to or bounded by the reference plant.

Some W PWR plants identified above (p. 4-2) incorporate designs that differ from the reference plant. These differences would not adversely change the results of the overfill events analyzed for the reference plant. Less-severe overfill events are expected for plants with larger steam generator volumes. Although other differences, such as operator training and procedures, the design of the level indication system, and alarms available to the operator, can alter the operator response time to an overfeed event, the review did not identify any plants that would have more severe overfill events.

(3) Conclusions

(a) Variations in the design of the automatic overfill protection system exist in other W PWR plants. The designs are the same as or better than the reference plant design (except as noted for three very early plant designs).

(b) Overfill transients in other W PWR plants are judged to be equal to or less severe than those analyzed for the reference plant.

(c) The ratio of steam generator volume to main feedwater flow rate at other W PWR plants are so similar to the reference plant ratio that the overfill analysis conducted on the reference plant is considered a bounding analysis applicable to other W PWR plants. (Although several plants provide different designs - so that some of the thermal-hydraulic characteristics discussed above are different from the reference plant characteristics - these differences do not change this conclusion.)

4.2.3 Overcool Events During Hot Shutdown and Full-Power Operation

(1) Control System Differences

Several control system failures were identified that could cause the condenser steam dump valves or the atmospheric dump valves (ADVs) to open. These failures can result in reactor vessel overcool events during full-power operation or hot-shutdown conditions.

All W PWR plants utilize similar ADV and condenser-steam dump valve control systems. Although the number of valves and valve capacities of these systems may differ at other W PWR plants, the overall valve capacity for 2-, 3-, and 4-loop plants are proportional to the plant power level. Transients resulting from failures in these systems at other W PWR plants were determined to be similar to those analyzed for the reference plant.

A majority of operating plants and plants under review for an operating license (i.e., 37 out of 52 W PWR plants) have incorporated lead/lag-compensated steamline pressure measurement in the steamline break protection systems. This control system can terminate steam flow through the condenser-steam dump valves by isolating the main steamlines on a low steamline pressure signal. This control design feature is not provided for the reference plant and is an improvement over the reference plant design. For W PWR plants utilizing this feature, overcool transients resulting from inadvertent opening of steam dump valves downstream of the main steam isolation valves (MSIVs) will be less severe than transients predicted for the reference plant.

In addition, most operating plants as well as plants of newer designs utilize arming circuits in the steam dump valve control system similar to circuits in the reference plant design. Multiple independent failures in these systems similar to those postulated for the reference plant, are needed to fail open all the steam dump valves. The initiating failure frequency for such events is very low.

Although one plant design (San Onofre Nuclear Generating Station, Unit 1) does not have MSIVs or a lead/lag-compensated steamline pressure control system, it does utilize arming circuits similar to those of the reference plant to prevent inadvertent opening of the dump valves.

Results and conclusions of analyses of the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system designs:

(a) Must automatically terminate the steam flow through the condenser steam dump valves by isolating the main steamlines on low steamline pressure (that is, must have a lead/lag-compensated steamline pressure control system, or equivalent) or

(b) Multiple independent control failures are needed to open all condenser steam dump valves (that is, provide arming circuits in the steam dump valve control systems similar to those in the reference plant).

(c) Administrative procedures are implemented to ensure that manual isolation of the ADVs can be accomplished in time to prevent severe overcooling, or multiple independent failures are required to open more than one ADV.

(2) Thermal-Hydraulic Differences

Most W PWR plant systems that can contribute to reactor vessel overcool transients are functionally similar. Although variations in the design exist at some plants (such as the number, type, and capacity of valves, and the number of steam generators), the variations are not significant when one considers the size of the plant. Major systems are sized in roughly the same proportions so that the overcool transients on other W PWR plants are expected to be similar to or bounded by transients analyzed for the reference plant. Several W PWR plants identified above (p. 4-2) incorporate designs that differ from the reference plant. Plants that have larger reactor vessel and steam generator volumes, like Yankee Rowe Nuclear Power Station, have larger cooling capacities and larger ratios for reactor coolant system volume to atmospheric-dump-valve (or steam-dump-valve) capacity and steam generator volume-to-atmospheric-dump-valve (or steam-dump-valve) capacity. Overcool transients resulting from inadvertent opening of the steamline PORV or condenser steam dump valves at these plants would be less severe than transients analyzed at the reference plant.

The following criteria were used to assess the generic applicability of this event at other W PWR plants: (a) Reactor coolant system volume to atmospheric or condenser steam dump valve capacity and (b) steam generator volume to atmospheric or condenser steam dump valve capacity ratios should be similar to or greater than these values for the reference plant.

Plants with thermal-hydraulic characteristics satisfying these criteria were determined to be similar to or bounded by the reference plant.

(3) Conclusions

(a) All W PWR plants provide adequate control systems to prevent overcool transients resulting from inadvertent opening of the steam dump valves to

the condenser. Most plants provide overcool transient protection better than that of the reference plant.

(b) Transients that could occur as a result of inadvertent opening of the condenser steam dump valves or atmospheric dump valves are expected to be equal to or less severe than those analyzed for the reference plant.

(c) Reactor coolant system volume to atmospheric dump valve or steam dump valve capacity and steam generator volume to ADV or steam dump valve capacity ratios at other W PWR plants are sufficiently similar that the overcool analysis conducted for the reference plant is a bounding analysis applicable to other W PWR plants.

Although several plants provide such different designs that some of the thermal-hydraulic characteristic discussed above are different from those for the reference plant, the differences would cause less severe transients and therefore do not adversely change the results of the overcool events analyzed for the reference plant.

4.2.4 Overpressure Events During Low-Temperature and Low-Pressure Shutdown or Startup Operating Conditions

Several control system failures were identified that could prevent pressurizer PORVs from opening. These failures in conjunction with events that would increase reactor coolant system (RCS) pressure can result in reactor vessel overpressure events.

(1) Control System Differences

Pressurizer PORV control systems at all W PWR plants are designed to conform to NRC Branch Technical Position RSB 5-2 (Denton, July 23, 1985) which requires the control systems for the pressurizer PORV valves to satisfy the single-failure criterion, and to be powered from reliable independent power supplies (not necessarily Class 1E). Some new plants provide additional control system improvements over the reference plant design by offering pressurizer PORV control system designs that conform fully to all the requirements of safety-related systems, so that additional failures would be needed to produce the transients analyzed for the reference plant. Control system designs on other W PWR plants are, therefore, very similar to or better than the reference plant designs.

(a) Results and conclusions of the analysis of the reference plant apply to other PWR plants if they meet the following criteria with respect to control system design:

- Pressurizer PORVs must be powered by reliable and independent power supplies and must be designed so that multiple independent failures are required to disable both PORVs.

- Administrative procedures are implemented to ensure that when one of the redundant pressurizer PORVs is rendered inoperable for a limited period of time during low-temperature operations, the remaining PORV can be opened manually.

Operator-induced procedural failures could also prevent both PORVs from opening during low-temperature and low-pressure conditions. These procedural failures are dependent on the adequacy of procedures used. Operating procedures at other plants were not reviewed to determine how many plants may be susceptible to the kind of procedurally induced conditions analyzed in the reference plant review. Variations in procedures at other plants could affect the frequency and severity of this procedurally induced transient. The emphasis on PORV-related events since the TMI-2 accident, however, has resulted in more operators becoming more aware of this type of transient.

(b) Results and conclusions of the analysis of the reference plant apply to other PWR plants if they meet the following criteria:

- The low-temperature overpressure (LTOP) system is removed from service during plant heatup before the RCS temperature is at or near the minimum pressurization temperature so that an LTOP condition can occur, or
- The ECCS is enabled during plant heatup before the RCS temperature is at or near the minimum pressurization temperature for the reactor vessel, or
- No other automatic pressure reduction capabilities exist to limit overpressure transients during low-temperature operations.

Under certain conditions, PWR plants are allowed to operate under limiting conditions for operation (LCOs), wherein redundant pressurizer PORV may be rendered inoperable for a finite period. If, during this time, the system is subjected to a pressure transient, the plant may be vulnerable to an overpressure event if a single failure in the available PORV control system can render the overpressure protection system inoperable. This scenario has been identified as a safety issue. Generic Issue 94 was identified to reevaluate the existing LTOP designs and to assess the need for additional improvements to the low-temperature overpressure protection system. This study is applicable to all PWRs with PORVs (Denton, July 23, 1985). By resolving this issue, insights may be gained to warrant modifications.

(2) Thermal-Hydraulic Differences

Because the major systems at W PWR plants are of roughly the same proportions, the overpressure transients at all W PWR plants are expected to be similar to or bounded by transients analyzed for the reference plant. Several W PWR plants identified above (p. 4-2) incorporate some designs that differ from the reference plant design. These differences, discussed in Section 4.2.1(b) (except for plants that have high capacity charging pumps), would not adversely change the results of the overpressure transients analyzed for the reference plant. For plants that utilize high-capacity charging pumps (higher than the reference plant design, like San Onofre Nuclear Generating Station, Unit 1), the overpressure transients induced by inadvertent initiation of the high-pressure injection could produce a more severe overpressure event than analyzed. Additional administrative procedures are used at these plants to lock out the isolation valves to the high-head pumps during shutdown conditions to preclude such

events so that additional independent failures would be required to cause similar or more severe events than analyzed for the reference plant. The following criteria were used to assess the generic applicability of these events to other W PWR plants:

(a) The ratio of RCS volume to normal cold shutdown letdown flow rate should be similar to or greater than that of the reference plant.

(b) Administrative procedures are implemented during startup or low-temperature, low-pressure operation to ensure that the pressurizer PORV low-pressure setpoint is not changed to the higher setpoint for normal operation before reaching the minimum pressurization temperature, or

(c) Other automatic pressure-reduction capabilities exist to limit the overpressure transients during LTOP operation.

(3) Conclusion

(a) Most pressurizer PORV control system designs at other W PWR plants are very similar to designs of the reference plant. The designs provide similar electrical independence.

(b) A few plants have better PORV control systems than the reference plant has, so additional multiple independent failures would be needed to produce similar scenarios analyzed for the reference plant.

(c) The thermal-hydraulic analyses conducted for the reference plant are applicable to other W PWR designs.

(d) Plants whose high-head injection pumps have a capacity higher than that of the reference plant provide additional lockout devices to prevent inadvertent initiation of the injection pumps during low-temperature operation.

4.2.5 Control System Failures Aggravating a Steam Generator Tube Rupture Event

Several control system failures were identified that could cause inadvertent opening (or failure to close once challenged) of the atmospheric steamline dump valves during an SGTR event. An ADV that fails to reclose during an SGTR event can result in more severe transients than those previously analyzed by W for an SGTR event.

All W PWR plants provide steamline ADV designs similar to that of the reference plant design. They rely on the operator to isolate the flow through these valves should the valves fail to close during an SGTR event. Although variations in the design of the ADVs may exist at other plants, these variations are not sufficient to modify the analysis performed for the reference plant design.

Results and conclusions of analysis of the reference plant apply to other W PWR plants if they meet the following criteria with respect to control system design:

(1) must have electrically initiated, air-operated ADVs
(2) require manual operator action to isolate flow through the ADVs

Conclusion

Transients at other W PWR plants that could occur as a result of inadvertent opening of the steamline ADVs are expected to be equal to or less severe than those analyzed at the reference plant.

4.3 B&W PWR Plants

The review of the B&W PWR reference plant identified potentially significant control system failures that could contribute to steam generator overfill events and reactor core overheating events. All other control system failures that were evaluated were determined to be bounded by the FSAR analysis. The failure mechanisms that contribute to these events are identified in Table 3.3.

The major contributors to these events were single and multiple control system failures that (1) initiated overfeed transients and failed the automatic feedwater pump trip system that would have terminated an overfill event and (2) caused a loss of electrical power to various sections of the integrated feedwater control system resulting in a feedwater underfeed condition that could lead to core overheating if proper operator action were not initiated.

It should be noted that about half of the B&W PWR plants currently operating incorporate an "820" integrated control system rather than a "721" integrated control system design utilized by the reference plant. Although the 820 and the 721 control systems are functionally similar, they differ significantly in the power supply configuration. Design differences, such as providing additional independence and power supply separation, were implemented by the individual utilities on the 820 systems in order to improve system reliability on a loss of power. However, for this review, the 721 and the 820 system were not compared in depth. To address the different transients resulting from a loss of power to the integrated control system (and other control systems), Bulletin 79-27 was issued by NRC's Office of Inspection and Enforcement to all licensees. The bulletin required all licensees to take certain action to ensure the adequacy of plant procedures for accomplishing cold shutdown upon a loss of power to any Class 1E or non-Class 1E bus supplying power for instruments and controls in systems used in attaining cold shutdown. The licensee's response and design modifications to comply with Bulletin 79-27 were considered and evaluated in the review of the reference plant. The staff did not verify satisfactory compliance with this bulletin for all other plants.

The following discussions summarize the generic applicability of the major transients identified in the reference plant to other B&W PWR plants.

4.3.1 Overfill Events Resulting From Failures in the Steam Generator, High-Level, Main-Feedwater, Trip System

(1) Control System Differences

Review of the main feedwater control systems at all B&W operating PWR plants and all new B&W designs currently under review for an operating license indicates that the 2-out-of-2, steam generator, high-level, main feedwater, trip system provided on the reference design is plant unique and not generically applicable.

All other B&W operating PWR plants have installed or have committed to install a safety-grade overfill protection system that will satisfy the single-failure criterion. (Arkansas Nuclear One, Unit 1, has committed to implement the new design by mid-1986; Rancho Seco Nuclear Generating Station, Unit 1, has committed to install its system by mid-1988; Three Mile Island Nuclear Station, Unit 1, will install its system in 1987; and Crystal River Nuclear Plant, Unit 3, has installed its system but has not yet implemented the trip system.) The initiating logic for these designs is either a 2-out-of-4 or a 1-out-of-2-taken-twice, steam generator, high-level, main feedwater, trip system. The trip system actuates redundant main feedwater isolation systems consisting of a main feedwater pump trip and a main feedwater isolation or control valve trip. One plant design currently under review for an operating license will use a safety-grade, 2-out-of-3, high-level, main feedwater, trip system. These plants provide (or will provide) additional redundancy, independence, and testing flexibility in their steam generator overfill protection system and they are expected to represent a significant improvement over the reference plant design when the installation is complete.

Results and conclusions of analyses of the reference plant apply to other B&W PWR plants if they meet the following criteria with respect to control system design:

(a) The automatic overfill protection is at least as reliable as the reference plant design. A single failure in the overfill protection system for the reference plant can negate the automatic overfill protection system.

(b) The main feedwater trip system must be operable during power operation, or administrative procedures must be implemented to ensure that manual feedwater trip can be accomplished in time to prevent overfill when the automatic feedwater trip system is not operable.

(2) Thermal-Hydraulic Differences

Most B&W PWR plant systems that could contribute to steam generator overfeed and overfill events are functionally similar. Variations in the designs exist at some plants, such as the type and capacity of main feedwater valves or pumps; these variations are not significant when considering to the overall size of the plant. Major systems are sized in roughly the same proportions so that the time to overfill on other B&W PWR plants is expected to be very similar or is bounded by the time predicted for the reference plant.

The following criterion was used to assess the generic applicability of this event on other plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than those of the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

(3) Conclusions

(a) Control systems for overfill protection for the main feedwater system for the reference plant is plant specific to the Oconee Nuclear Station

design (i.e., Units 1, 2, and 3). The control systems for overfill protection are not as reliable as those provided or planned to be provided at all other B&W PWR plants.

(b) All other B&W PWR plants provide (or have committed to provide) improved safety-grade control systems for steam generator overfill protection systems for the main feedwater system. These systems consist of either a 2-out-of-4 or a 1-out-of-2- taken-twice or a 2-out-of-3 steam generator, high-level trip. Although there are theoretical reliability differences between these systems, they are outweighed by the improvements in overall reliability and operational flexibility allowed by such systems. All are thus adequate for overfill protection. It should be noted that until these modifications are completed some of the plants are currently operating with no overfill protection.

(c) Steam generator volume to main feedwater flow rate and steam generator volume to auxiliary feedwater flow rate ratios on other B&W PWR plants are similar to the reference plant ratios; thus the overfill analysis conducted on the reference plant is a bounding analysis applicable to other B&W PWR plants.

4.3.2 Overheat Events Resulting From Steam Generator Dryout

Several control system failure scenarios were identified that could result in steam generator dryout on a partial loss of electrical power to the feedwater control system. Such events could lead to reactor core overheating if adequate feedwater flow is not established within 30 minutes of a steam generator dryout and high-pressure injection (HPI) is not initiated within 60 minutes. Losses of electrical power to the "hand control" (i.e., manual control) circuit during manual mode of operation or to the "auto control" circuit during the automatic mode of operation were identified as major contributors.

(1) Control System Differences

Half of the operating B&W PWR plants have an 820 integrated control system rather than a 721 integrated control system used at the reference plant. Only four plants (Oconee Nuclear Station, Units 1, 2, and 3, and Three Mile Island Nuclear Station, Unit 1) use 721 systems. Electric power distributions in the 820 system are different from the distributions in 721 system. A detailed review of the 820 system was not performed to determine if a credible partial loss of power to the integrated control system could cause similar events; however, all other plants (including TMI-1) incorporate separate control circuits that automatically initiate auxiliary feedwater flow on low steam generator level. These circuits represent an improved design that mitigates a steam generator dryout scenario that is postulated for the reference plant.

Results and conclusions of analyses of the reference plant apply to other B&W PWR plants if they meet the following criterion with respect to control system design: Auxiliary feedwater flow is not automatically initiated on low steam generator water level. (Plants in which AFW is automatically initiated on low steam generator level are less susceptible to steam generator dryout and, therefore, represent an improvement over the reference design.)

(2) Thermal-Hydraulic Differences

Variation in the designs exist at some plants, such as type and capacity of the feedwater valves or pumps. These variations are not significant when considering the overall size of the plant. Major systems are sized in roughly the same proportions so that the time of steam generator dryout at other B&W plants is expected to be similar to or bounded by the time to dryout predicted for the reference plant. The following criteria were used to assess the generic applicability of this event to other B&W plants:

(a) The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to these values for the reference plant.

(b) Power to volume ratios should be similar to these values for the reference plant.

Plants with thermal-hydraulic characteristics satisfying these criteria were judged to be similar to the reference plant.

(3) Conclusions

(a) All other B&W PWR plants provide control system designs to initiate auxiliary feedwater on steam generator low water level to prevent steam generator dryout on loss of main feedwater. This design feature represents an improvement over the reference plant design.

(b) Power to flow, power to feedwater flow rate, and steam generator volume to main feedwater flow ratio at other B&W PWR plants are similar to values for the reference plant, thus the steam generator dryout analysis conducted for the reference plant is similar to or is a bounding analysis for other B&W PWR plants.

(c) The overheating event scenario analyzed for the reference plant is not directly generically applicable but bounds overheating events at other B&W PWR plants.

4.4 CE PWR Plants

The review of the CE PWR reference plant identified several potentially significant control system failures that could contribute to (1) steam generator overfill events,(2) a reactor core overheating event, and (3) an overcooling event that could lead to a potential pressurized thermal shock event in a plant with a vulnerable pressure vessel.

All other control system failures that were evaluated were determined to be bounded by the FSAR analysis. The failure mechanisms that contributed to these events are identified in Table 3.4.

The major contributors to these events were single and multiple control system failures that initiated overfeed transients or prevented atmospheric dump valves or Turbine bypass valves from opening on demand, and incorrect operator actions to open the pressurizer PORVs when needed.

The following discussions summarize the generic applicability of the major transients identified in the reference plant to other CE PWR plants.

4.4.1 Overfill Events Resulting From Operator Errors During a Steam Generator Overfeed Event

(1) Control System Differences

On all CE PWR plant designs, no automatic, steam generator, high-water-level signals trip the main feedwater pumps. In the event of an overfeed, a steam generator, high-water-level signal will automatically trip the main steam turbine. A turbine trip signal will trip the reactor, shut the feedwater valves, and open the startup feedwater valves to 5% flow.

This trip system can limit the frequency of steam generator overfill events, but operator action is still required to trip the main feedwater pumps to prevent overfill. If the operator does not manually trip the feedwater pumps, a single failure in the feedwater control system can cause the steam generator to overfill.

The results and conclusions of analysis on the reference plant apply to other CE PWR plants if they meet the the following criterion with respect to control system design: All main feedwater flow is not automatically isolated on a steam generator, high-water-level signal. Plants with automatic overfill control circuits would be more resistant to overfill than the reference plant would be.

(2) Thermal-Hydraulic Differences

Variations in design exist at some plants. These variations include type and capacity of feedwater valves and pumps. These variations are not significant with regard to steam generator fill times when considering the relative size of the plants. Major systems are sized in roughly the same proportions so that the time to overfill at all other CE PWR plants is expected to be similar or bounded by the time to overfill predicted for the reference plant.

Several CE PWR plants incorporate designs that are different from the reference plant design. These design differences include (a) the use of charging pumps with a discharge head higher than the reference plant design and (b) no pressurizer PORVs. These design differences would not change the conclusions for overfill events analyzed for the reference plant. Although other differences, such as operator training and procedures and design of the level indication system and alarms available to the operator, will alter operator response time to respond to an overfill event, the review did not identify any plants with characteristics that would cause more severe overfill events.

The following criterion was used to assess the generic applicability of this event to other CE PWR plants: The ratio of steam generator volume to main feedwater flow rate and the ratio of steam generator volume to the auxiliary feedwater flow rate should be similar to or greater than these values for the reference plant.

Plants with thermal-hydraulic characteristics satisfying this criterion were determined to be similar to the reference plant.

(3) Conclusions

(a) The feedwater control system designs on all CE PWR plants are similar to feedwater control system design for the reference plant.

(b) There are no automatic steam generator, high-level, feedwater-pump, trip systems; manual operator action is required to trip the feed pumps or close isolation valves to prevent overfill.

(c) The ratios of steam generator volume to main feedwater flow rate at all CE PWR plants are similar to such ratios at the reference plant, thus the overfill analysis conducted for the reference plant is considered applicable to other CE PWR plants.

4.4.2 Overheat Events and Possible Pressurized Thermal Shock Events Resulting From Operator Errors During Small-Break Loss-of-Coolant Accidents

Several failure scenarios were identified for specifically sized, small-break, loss-of-coolant accidents (SBLOCAs) that could lead to eventual core dryout and fuel damage if the operator does not take proper action to depressurize the reactor coolant system to (1) maintain adequate high-pressure injection flow or (2) avoid reaching R_TNDT (reference temperature nil ductility transition) limits.

(1) Control System Differences

For the reference plant, manual operation of the atmospheric dump valves (ADVs) or the turbine bypass valves (TBVs) or both may be required to depressurize the primary system during SBLOCAs to maintain adequate high-pressure injection flow. Operator use of the pressurizer PORVs or pressurizer auxiliary sprays could also be used to depressurize the primary system if the ADVs or the TBVs or both are not available or if the R_TNDT limits for the reactor vessel are exceeded.

Failures that could keep the ADVs or the TBVs from opening on demand include loss of power or loss of instrument air to the valves. For the reference plant under LOCA conditions, a safety-injection signal isolates service water flow to the air compressors that supply operation air to the ADVs and the TBVs. Loss of service water could result in a failure of the air system. This design is similar to the design of other CE PWR plants. Although an operator of the reference plant can manually transfer control of the ADV to the auxiliary shutdown panel and can provide air to the valves from the salt-water-cooled air compressor, emergency procedures for the reference plant do not instruct the operator to perform this task.

Results and conclusions of analysis of the reference plant apply to other CE PWR plants if they meet the following criteria with respect to administrative procedures or control system design:

(a) Air supply to ADVs or to the TBVs is lost during SBLOCA conditions. (At the reference plant, automatic isolation of service water to instrument air compressors is initiated during LOCA conditions so that the ADVs or the TBVs are rendered inoperable. Plants that continue to supply instrument air to the ADVs under LOCA conditions are protected against this type of event.)

(b) Administrative procedures do not clearly instruct the operators to provide operating air to the ADV or the TBVs from an alternate source in the event that service water flow is isolated to the main instrument air compressors (if administrative procedures exist, plants are less susceptible to overheat events of this type), and

(c) An alternate, compressed-air source to the ADVs or TBVs is available.

(2) Thermal-Hydraulic Differences

Several CE PWR plants incorporate designs that are different from the reference plant design. These design differences include (a) the use of high-head, safety-injection pumps with higher heads than the reference plant has and (b) some CE PWR plants do not have pressurizer PORVs. The use of higher head injection pumps will significantly change the analyzed failure scenarios. Higher head pumps will be able to inject water into the reactor vessel at higher pressures, so that specifically sized SBLOCA events analyzed for the reference plant would be significantly less severe.

The following criterion was used to assess the generic applicability of this event on other CE PWR plants: The shutoff pressure of the high-head pumps should be similar to or less than the reference plant design safety injection.

Plants satisfying this criterion were determined to be similar to the reference plant. Plants with higher head safety injection pumps were determined to have less severe transients than analyzed.

(3) Conclusions

(a) Seven of the fifteen CE PWR plants have similar high-head pressure injection pump systems, thus failure scenarios analyzed on the reference plant are generically applicable.

(b) Eight of the fifteen CE PWR plants have substantially higher high-head pressure injection pumps, so that administrative procedures to depressurize the primary system are not as critical for these eight plants as for the reference plant.

(c) Seven of the eight CE PWR plants that have high-head pressure injection pumps do not have pressurizer PORVs. For these plants, auxiliary pressurizer spray systems are used to control pressurizer pressure. This design difference does not significantly change the conclusions reached in item b, above.

5 SUMMARY AND CONCLUSIONS

The resolution of any safety issue requires that the nature of the concern be clearly described. Concerns described as general subject areas (such as common-cause failures, operator errors, sabotage, and undetected failures) can prove to be so broad that almost every conceivable safety issue could fall within the concern, and thus an issue would prove to be unmanageable. Therefore, to proceed with a resolution of the concern expressed as "safety implications of control systems," the NRC staff developed a set of limitations and assumptions to attempt to focus on the safety concern. The staff also decided to take advantage of other ongoing efforts. Thus, if some aspects that might be considered to have control system safety implications were better addressed by these other efforts, the scope of USI A-47 was modified, avoiding duplication of effort. As a result, a number of concerns (such as: (1) effects of seismic events on control systems, (2) dynamic effects on plant safety resulting from water entering the main steamlines, and (3) reduction in the frequency of integrated-control-system-induced transients in B&W PWR plants) were left to be addressed outside USI A-47. The limitations and assumptions identified in this report are crucial to understanding the scope of the issue and its resolution.

On the basis of the limitations and assumptions, a number of tasks were defined. These tasks were structured to: (1) make use of the operating experience of actual events, (2) take advantage of previous control system studies, (3) take advantage of the staff requirements identified in the TMI-2 Action Plan (NUREG-0660), (4) evaluate the safety significance of control system failures, and (5) evaluate the safety benefit and cost effectiveness of potential corrective measures.

Because the initiating events and the frequency of control system failures are for the most part plant specific, the risk estimates that are used to evaluate safety significance were difficult to extrapolate to other plants. The safety benefit derived for the reference plant and extrapolated to other plants is based both on qualitative insights and quantitative analysis. The generic applicability analysis is also based on qualitative analysis and deterministic arguments.

On the basis of the technical work completed by the staff and NRC contractors, the following conclusions have been reached:

(1) Control system failures are dependent on individual plant characteristics such as power supply configurations and maintenance. The control system designs between the plants supplied by the same nuclear steam supply system (NSSS) vendor are functionally similar enough that the transients resulting from the failure of the same type of non-safety-grade system on the different plants will produce similar transients (see Section 4, "Generic Applicability," for exceptions).

(2) Control system failures have occurred that resulted in complex transients. Improvements made after the TMI-2 accident in the design of the auxiliary feedwater system and in operator information and training should greatly aid in the recovery actions in the future.

(3) Plant transients resulting from control system failures can be adequately mitigated by the operators provided the failures do not compromise proper operation of the minimum number of protection system channels required to trip the reactor and initiate the safety systems if such initiation is required.

(4) Control system failure scenarios have been identified that could potentially lead to reactor vessel/steam generator overfill events, core overheat events, and overpressure events.

(5) Transients or accidents resulting from or aggravated by control system failures (except those noted in this report that can contribute to reactor vessel/steam generator overfill or core overheat events) are less severe and therefore are bounded by the transients and accidents identified in the FSAR analysis.

(6) PWR plant designs having redundant commercial grade (or better) overfill protection systems that satisfy the single-failure criterion are considered to adequately preclude water ingress into the main steamlines.

(7) BWR plant designs with commercial grade (or better) overfill protection systems are considered to adequately preclude water ingress into the main steamlines.

(8) PWR plant designs that provide automatic initiation of the auxiliary feedwater flow on low steam generator level are considered to adequately preclude core overheating.

6 REFERENCES

Alter, J., and D. Okrent, "The Contribution of Control Systems in LWR Safety," University of California, Los Angeles, 1983.

Babcock and Wilcox Owners Group, BAW 1564, "Integrated Control System Reliability Analysis," August 1979.

Denton, H., NRC, Memorandum to R. Bernero, "Schedule for Resolving and Completing Generic Issue No. 94, 'Additional Low Temperature Overpressure Protection for Light Water Reactors'," July 23, 1985.

Denton, H., Memorandum to V. Stello, "Staff Actions Resulting from the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," April 25, 1986.

Dircks, W., NRC, Memorandum to NRC Directors, "Staff Actions Resulting from the Investigation of the June 8, Davis-Besse Event (NUREG-1154)," August 5, 1985.

Miraglia, F., NRC, Memorandum to NRR Directors, "Staff Actions Resulting from the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," September 4, 1986.

Stello, V., NRC, Memorandum to H. Denton, "Staff Actions Resulting from the Investigation of the December 26, 1986 Incident at Rancho Seco (NUREG-1195)," March 13, 1986.

Tucker, H., BWOG, Letter to D. Crutchfield, NRC, "B&W Owners Group Plant Reassessment," May 15, 1986.

---, NUREG-0153, "Staff Discussions of Twelve Additional Technical Issues Raised by Responses to November 3, 1976 Memorandum From Director, NRR, to NRR Staff," December 1976.

---, NUREG-0460, "Anticipated Transients Without Scram for Light Water Reactors," Vols. 1 and 2, April 1978; Vol. 3, December 1978; Vol. 4, March 1980.

---, NUREG-0660, "NRC Action Plan Developed as a Result of the TMI-2 Accident," Vols. 1 and 2, May 1980.

---, NUREG-0667, "Transient Response of Babcock & Wilcox-Designed Reactors," May 1980.

---, NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

---, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition, July 1981.

---, NUREG-0933, "A Prioritization of Generic Safety Issues," Main Report and Supplements 1-6, August 1987.

---, NUREG-1070, "NRC Policy on Future Reactor Designs," July 1985.

---, NUREG-1154, "Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985," July 1985.

---, NUREG-1177, "Safety Evaluation Report Related to the Restart of Davis-Besse Nuclear Power Station, Unit 1, Following the Event of June 9, 1985," June 1986.

---, NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," February 1986.

---, NUREG-1218 (Draft for Comment), "Regulatory Analysis for Proposed Resolution of USI A-47, Safety Implications of Control Systems," April 1988.

---, NUREG/CR-3958 (PNL-5767), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.

---, NUREG/CR-3991 (ORNL/TM-9383), "Failure Modes and Effects Analysis (FMEA) of the ICS/NNI Electric Power Distribution Circuitry at the Oconee-1 Nuclear Plant," October 1985.

---, NUREG/CR-4047 (ORNL/TM-9444), "An Assessment of the Safety Implications of Control Systems at the Oconee 1 Nuclear Power Plant, Final Report," March 1986.

---, NUREG/CR-4262 (EGG-2394), "Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor," Vols. 1 and 2, May 1985.

---, NUREG/CR-4265 (ORNL/TM-9640), "An Assessment of the Safety Implications of Control Systems at the Calvert Cliffs-1 Nuclear Plant," Vol. 1, Main Report, April 1986; Vol. 2, Appendices, July 1986.

---, NUREG/CR-4326 (EGG-2405), "Effects of Control System Failures on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor," Vol. 1, August 1985; Vol. 2, October 1985.

---, NUREG/CR-4385 (PNL-5543), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor," November 1985.

---, NUREG/CR-4386 (PNL-5544), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor," Pacific Northwest Laboratory, December 1985.

---, NUREG/CR-4387 (PNL-5545), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor," December 1985.

---, NUREG/CR-4449 (ORNL/TM-9868), "A PWR Hybrid Computer Model for Assessing the Safety Implications of Control Systems," March 1986.

---, NUREG/CR-4758 (ORNL/TM-10236), "A RETRAN Model of the Calvert Cliffs-1 Pressurized Water Reactor for Assessing the Safety Implications of Control Systems," March 1987.

---, Office for Analysis and Evaluation of Operational Data, "AEOD Observations and Recommendations Concerning the Problem of Steam Generator Overfill and Combined Primary and Secondary Blowdown," December 17, 1980.

---, Office of Inspection and Enforcement, Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation," November 30, 1979.

---, SECY-82-465, "Pressurized Thermal Shock (PTS)," November 23, 1982.

---, ORNL/NRC/LTR-86/19, Letter Report, "Generic Extensions to Plant Specific Findings of the Safety Implications of Control Systems (ORNL) Program."

APPENDIX A

OTHER RELATED STUDIES, PROGRAMS, AND ISSUES

A number of ongoing NRC and industry programs are related to USI A-47. These programs are discussed here and summarized in Table A1.

(1) Generic Issues in NUREG-0933

As specifically identified in NUREG-0933, Generic Issues 70 and 94 dealing with overpressure protection may require modifications to existing control systems. The staff concluded that resolution of these issues should proceed via the more focused review specified for these generic issues.

(2) Seismic Qualification of Equipment in Operating Plants, USI A-46

Ongoing NRC and industry programs are evaluating the seismic ruggedness and operability of control and protection grade design equipment during basis seismic events. Data from actual experience during seismic events (including recent earthquakes in Chile and Mexico) are being evaluated to assess the seismic capability of electrical and mechanical equipment needed to safely shut down the plant. Equipment used in non-safety-grade control systems that interface with safety-grade equipment or that are used in achieving and maintaining hot shutdown are being evaluated to assure that their operability (or lack thereof) does not compromise the plant's ability to achieve and maintain hot shutdown during or after a seismic event. All control system components and instruments are included in the USI A-46 scope by type if not explicitly reviewed. As part of the USI A-46 scope, the current review is evaluating two plant designs (i.e., Zion and Nine Mile Point Unit 1), focusing on equipment installation, its function, and its actual location. Once the methodology and review procedures are established, the review will extend to all other operating plants in the USI A-46 scope (which includes 70 operating plants).

(3) Reactor Vessel/Steam Generator Overfill

In separate evaluations, staff is investigating the consequences of water ingress in the main steamlines resulting from overfeed transients or steam generator tube rupture (SGTR) events. These evaluations include (a) analysis of the potential waterhammer conditions that could degrade steamline integrity, (b) assessment of the adequacy of existing emergency procedures for operator actions needed to mitigate SGTR and prevent overfill, and (c) radiological offsite dose calculations from an SGTR event. These activities are being evaluated under Generic Issue 135.

(4) Babcock and Wilcox Design Reexamination

A comprehensive B&W Owners Group study (Tucker, May 15, 1986) has been initiated to reassess all B&W PWR plant designs including, but not limited to, the integrated control system, support systems such as power supplies, and maintenance.

The purpose of this reexamination is to improve the reliability of the B&W PWR plants by (a) reducing the number of reactor trips caused by non-safety-grade control and support systems or by operator or maintenance errors and (b) improving response to plant transients. The NRC staff is monitoring this comprehensive study. Recommended actions for design modifications (if any), for maintenance, and for changes to operating procedures developed for the utilities by the owners group will be coordinated with the staff through NRC's Division of Engineering and System Technology. This effort is closely coordinated with the USI A-47 effort, but is proceeding independently. Any requirements developed will be implemented independent of USI A-47.

(5) Staff Actions Resulting From the Investigation of the December 26, 1985 Incident at Rancho Seco

Generic and plant-specific actions resulting from the investigation of the Rancho Seco incident (see NRC, NUREG-1195) were identified in part in a memorandum from V. Stello to H. Denton, dated March 13, 1986, and in a subsequent response memorandum, dated April 25, 1986. Several other memoranda have been issued subsequent to the April 25, 1986 response related to the identified issues. These memoranda are listed in the September 4, 1986 memorandum from F. Miraglia to the various directors of NRR. The activities discussed in these memoranda are being pursued by the NRC staff and are currently being reevaluated by the B&W Owners Group (BWOG). The major activities are summarized below, and are being resolved on a separate schedule independent from USI-A47.

(1) Regarding completeness of actions taken with respect to BAW-1564 (Failure Modes and Effects Analysis of the ICS) and the ORNL review of it, the BWOG has been asked to reevaluate BAW-1564 and to describe its plans to address the ORNL concerns. The staff will ensure that the recommendations in BAW-1564 and the ORNL review are reconsidered regarding their applicability, appropriateness, and implementation status at each B&W-designed operating reactor.

(2) The staff has asked the BWOG, and BWOG has agreed, to reevaluate IE Bulletin 79-27 regarding the consequences of a loss of power to the instrumentation and control systems for all of the B&W-designed operating plants.

In retrospect, the staff could have done more in reviewing licensee responses to Bulletin 79-27 by focusing its resources on a more detailed review of the B&W-designed plants. The staff is now giving more attention and resources to problem plants. The staff will thoroughly review the BWOG reevaluation of Bulletin 79-27.

(3) With regard to atmospheric dump valves (ADVs) and turbine bypass valves (TBVs) opening on loss of integrated control system (ICS) power, the staff has met with the BWOG and determined that only Rancho Seco has the ADV problem and only Rancho Seco and Arkansas Nuclear One Unit 1 (ANO-1) have the TBV problem. Rancho Seco has already redesigned the ADV and TBV controls to eliminate the problem, and the staff will review the modifications before Rancho Seco restarts. ANO-1 modified its TBV controls during the August 1986 refueling. The modified design prevents the TBV from automatically opening on a loss of power in the ICS.

(4) The staff has conducted a survey of completeness of actions taken with respect to NUREG-0667 recommendations by the staff and by licensees of each B&W-designed operating reactor. The survey shows that 90% of the related staff requirements have been implemented; the rest will be complete by the end of 1987. The staff is planning to review the prioritization of certain lower-priority recommendations that were not required earlier. The Rancho Seco licensee and the BWOG are reviewing the recommendations as part of the Rancho Seco recovery and B&W-design reassessment programs, respectively.

(5) In connection with the partial loss of the non-nuclear instrumentation (NNI) system at Rancho Seco in 1984, in the near future the staff plans to complete its review of the BWOG submittal (dated January 1985) evaluating the generic aspects of that event. In addition, Rancho Seco staff and the BWOG are reviewing this event as part of the recovery and design reassessment programs, respectively.

(6) Staff Actions Resulting From the June 6, 1985 Incident at Davis-Besse

Generic and plant-specific actions resulting from the investigation of the Davis-Besse incident (see NRC, NUREG-1154) have been identified in a memorandum from W. Dircks to the Directors of NRC, dated August 5, 1985. Short-term, plant-specific items have been addressed and the resolution is described in the "Safety Evaluation Report Related to Restart of Davis-Besse Nuclear Power Station" (see NRC, NUREG-1177). A number of potential generic issues were also identified. These issues include possible deficiencies in the design, construction, or operation of several or a class of nuclear power plants. The staff did not identify a need for any immediate staff action of a generic nature related to these issues. They have, however, been designated for review as part of Generic Issues 122 through 125. These issues are to be evaluated and resolved on a schedule consistant with their priority designation. Currently, the staff is completing the prioritization of these issues. Their status and priority level is provided in NUREG-0933. Resolution of these issues is being pursued on a separate schedule independent from USI A-47.

(7) Systems Interactions (USI A-17)

Potentially undesirable interactions between plant systems, components, and structures were evaluated under USI A-17. These evaluations include identification of interdependencies between safety-grade protection systems and systems not related to safety, including non-safety-grade control systems.

Table A1 Summary of USI A-47 related studies, programs, and issues

Issue	Subject	Estimated completion schedule
GI-70	PORV and block valve reliability	Late 1988
GI-94	Low-temperature overpressure protection for light-water reactors	Late 1988
USI A-46	Seismic qualification of components	Mid 1991 (plant-specific implementation)
GI-135	Water ingress to main steamlines (overfill)	Late 1989
B&W plant reexamination	BWOG reevaluation to minimize challenges to protection systems and improve mitigation of complex transients	Early 1988
Staff actions resulting from Rancho Seco Dec. 26, 1985 incident	Included as part of BWOG reevaluation	Early 1988
Staff actions resulting from Davis-Besse June 6, 1985 incident	NUREG- 1177 (short-term actions)	Completed June 1986
	GI-122 (initiating feed and bleed)	Mid 1988
	GI-124 (AFW system reliability)	Mid 1988
	GI-125 (reevaluate design design to automatically isolate feedwater from the steam generator	Mid 1989
USI-A-17	Systems interactions	Mid 1989

APPENDIX B

SUMMARY OF THE PRINCIPAL DOCUMENTS USED FOR USI A-47 STUDY

The following are summaries of the principal documents underlying the proposed resolution of USI A-47.

(1) Draft NUREG-1217, "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-47."

This report presented the technical findings and summarizes the work performed on USI A-47 by the U.S. Nuclear Regulatory Commission (NRC) and its contractors: Pacific Northwest Laboratory (PNL), Idaho National Engineering Laboratory (INEL), and Oak Ridge National laboratory (ORNL). Summaries and staff conclusions regarding other related work, such as generic applicability and operating experience survey, are also presented.

From the technical findings presented in this report, the staff formulated the resolution of USI A-47.

(2) Draft NUREG-1218, "Regulatory Analysis for Proposed Resolution of USI A-47 Safety Implications of Control Systems."

This report presents a summary of the regulatory analysis conducted by the NRC staff to evaluate the value impact of alternatives for resolution of USI A-47. The proposed resolution presented in this USI A-47 study is based on these analyses.

(3) NUREG/CR-4262, "Effects of Control System Failures on Transients and Accidents at a General Electric Boiling Water Reactor" (Vols. 1 and 2). (See summary for NUREG/CR-4326.)

(4) NUREG/CR-4326, "Effects of Control System Failures on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor" (Vols. 1 and 2).

These two reports (numbers 3 and 4) summarize the work performed on USI A-47 by INEL. Summaries of failure modes and effects analysis, computer analysis, recorded plant occurrences, and probabilistic assessment of significant control system failure frequencies are provided. In addition, the contractor presents its conclusions and recommendations.

From the technical findings presented in these two reports, the staff formulated the resolution of USI A-47 for General Electric and Westinghouse plants.

(5) NUREG/CR-4047, "An Assessment of the Safety Implications of Control at the Oconee 1 Nuclear Plant." (See summary for NUREG/CR-4265.)

(6) NUREG/CR-4265, "An Assessment of the Safety Implications of Control Systems at the Calvert Cliffs 1 Nuclear Power Plant" (Vols. 1 and 2).

These two reports (numbers 5 and 6) summarize the work performed on USI A-47 by ORNL. Summaries of failure modes and effects analysis, computer analysis, recorded plant occurrences, and probabilistic assessment of significant control system failure frequencies are provided. In addition, the contractor presents its conclusions and recommendations.

From the technical findings presented in these two reports, the staff formulated the resolution of USI A-47 for Babcock and Wilcox Company and Combustion Engineering plants.

(7) NUREG/CR-4385, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor." (See summary for NUREG/CR-3958.)

(8) NUREG/CR 4386, "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor." (See summary for NUREG/CR-3958.)

(9) NUREG/CR-4387, "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor." (See summary for NUREG/CR-3958.)

(10) NUREG/CR-3958, "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor."

These four reports (numbers 7-10) summarize the work performed on A-47 by PNL. Probabilistic risk analyses and estimates of core-melt frequencies and public risk associated with control system failures in Westinghouse, Babcock and Wilcox, General Electric, and Combustion Engineering reactors are presented. In addition, value/impact analyses of possible modifications to prevent control system failures are presented. These analyses are based on the control system failures identified by INEL and ORNL.

From the technical findings presented in these four reports, the staff developed the regulatory analysis for USI A-47.

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG-1217

2. TITLE AND SUBTITLE
Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants
Technical Findings Related to Unresolved Safety Issue A-47
Draft Report for Comment

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: March YEAR: 1988

5. AUTHOR(S)
A. J. Szukiewicz

6. DATE REPORT ISSUED
MONTH: April YEAR: 1988

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Same as 7, above.

11a. TYPE OF REPORT
Draft Report for Comment

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

This report summarizes the work performed by the Nuclear Regulatory Commission staff and its contractors, Idaho National Engineering Laboratories (INEL), Oak Ridge National Laboratory (ORNL), and Pacific Northwest Laboratory (PNL), leading to the proposed resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems".

An in-depth evaluation was performed on non-safety-grade control systems (see Section 1) that are typically used during normal plant operation on four nuclear steam system (NSS) plants: a General Electric Company (GE) boiling-water reactor (BWR), a 3-loop Westinghouse (W) pressurized-water reactor (PWR) design, a once-through steam generator PWR designed by Babcock & Wilcox Co. (B&W), and a Combustion Engineering (CE) PWR design.

This report describes the technical studies performed by the laboratories, the NRC staff assessment of the results, the generic applicability of the evaluations, and the technical findings resulting from these studies.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS
Unresolved Safety Issue
A-47
Control Systems

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

*U.S. GOVERNMENT PRINTING OFFICE: 1988-202-292:80056

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE & FEES PAID
USNRC
PERMIT No. G-67

DRAFT REPORT